EXHIBIT A

Supreme Court of Pennsylvania

Court of Common Pleas
Civil Cover Sheet

LACKAWANNA County

For Prothonotary Use Only:	TIME STAMP
Docket No: 23 CV 1911	

The information collected on this form is used solely for court administration purposes. This form does not supplement or replace the filing and service of pleadings or other papers as required by law or rules of court.

SECTION A

Commencement of Action:
☒ Complaint ☐ Writ of Summons ☐ Petition
☐ Transfer from Another Jurisdiction ☐ Declaration of Taking

Lead Plaintiff's Name:	Lead Defendant's Name:
JANE DOE, ET AL.	GEISINGER HEALTH
Are money damages requested? ☒ Yes ☐ No	Dollar Amount Requested: (check one) ☐ within arbitration limits ☒ outside arbitration limits
Is this a *Class Action Suit?* ☒ Yes ☐ No	**Is this an *MDJ Appeal?*** ☐ Yes ☒ No

Name of Plaintiff/Appellant's Attorney: _____

☐ **Check here if you have no attorney (are a Self-Represented [Pro Se] Litigant)**

SECTION B

TORT *(do not include Mass Tort)*
- ☐ Intentional
- ☐ Malicious Prosecution
- ☐ Motor Vehicle
- ☐ Nuisance
- ☐ Premises Liability
- ☐ Product Liability *(does not include mass tort)*
- ☐ Slander/Libel/ Defamation
- ☒ Other: Pennsylvania Wire Tap Act, 18 Pa. C.S.A. Section 5725

MASS TORT
- ☐ Asbestos
- ☐ Tobacco
- ☐ Toxic Tort - DES
- ☐ Toxic Tort - Implant
- ☐ Toxic Waste
- ☐ Other:

PROFESSIONAL LIABLITY
- ☐ Dental
- ☐ Legal
- ☐ Medical
- ☐ Other Professional:

CONTRACT *(do not include Judgments)*
- ☐ Buyer Plaintiff
- ☐ Debt Collection: Credit Card
- ☐ Debt Collection: Other
- ☐ Employment Dispute: Discrimination
- ☐ Employment Dispute: Other
- ☐ Other:

REAL PROPERTY
- ☐ Ejectment
- ☐ Eminent Domain/Condemnation
- ☐ Ground Rent
- ☐ Landlord/Tenant Dispute
- ☐ Mortgage Foreclosure: Residential
- ☐ Mortgage Foreclosure: Commercial
- ☐ Partition
- ☐ Quiet Title
- ☐ Other:

CIVIL APPEALS
Administrative Agencies
- ☐ Board of Assessment
- ☐ Board of Elections
- ☐ Dept. of Transportation
- ☒ Statutory Appeal: Other
- ☐ Zoning Board
- ☐ Other:

MISCELLANEOUS
- ☐ Common Law/Statutory Arbitration
- ☐ Declaratory Judgment
- ☐ Mandamus
- ☐ Non-Domestic Relations Restraining Order
- ☐ Quo Warranto
- ☐ Replevin
- ☐ Other:

2023 MAY -4 A 10:45 MAURA B. KELLY PROTHONOTARY LACKAWANNA COUNTY PA

Updated 1/1/2011

NOTICE

Pennsylvania Rule of Civil Procedure 205.5. (Cover Sheet) provides, in part:

Rule 205.5. Cover Sheet

(a)(1) This rule shall apply to all actions governed by the rules of civil procedure except the following:

(i) actions pursuant to the Protection from Abuse Act, Rules 1901 et seq.

(ii) actions for support, Rules 1910.1 et seq.

(iii) actions for custody, partial custody and visitation of minor children, Rules 1915.1 et seq.

(iv) actions for divorce or annulment of marriage, Rules 1920.1 et seq.

(v) actions in domestic relations generally, including paternity actions, Rules 1930.1 et seq.

(vi) voluntary mediation in custody actions, Rules 1940.1 et seq.

(2) At the commencement of any action, the party initiating the action shall complete the cover sheet set forth in subdivision (e) and file it with the prothonotary.

(b) The prothonotary shall not accept a filing commencing an action without a completed cover sheet.

(c) The prothonotary shall assist a party appearing pro se in the completion of the form.

(d) A judicial district which has implemented an electronic filing system pursuant to Rule 205.4 and has promulgated those procedures pursuant to Rule 239.9 shall be exempt from the provisions of this rule.

(e) The Court Administrator of Pennsylvania, in conjunction with the Civil Procedural Rules Committee, shall design and publish the cover sheet. The latest version of the form shall be published on the website of the Administrative Office of Pennsylvania Courts at www.pacourts.us.

JANE DOE INDIVIDUALLY AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED, Plaintiff, v. GEISINGER HEALTH and DOE ENTITIES 1-99, Defendants.	IN THE COURT OF COMMON PLEAS OF LACKAWANNA COUNTY, PENNSYLVANIA CIVIL ACTION - LAW Case No. 23cv1911 JURY TRIAL DEMANDED

NOTICE

NOTICE

You have been sued in court. If you wish to defend against the claims set forth in the following pages, you must take action within twenty (20) days after this complaint and notice are served, by entering a written appearance personally or by attorney and filing in writing with the court your defenses or objections to the claims set forth against you. You are warned that if you fail to do so the case may proceed without you and a judgment may be entered against you by the court without further notice for any money claimed in the complaint or for any other claim or relief requested by the plaintiff. You may lose money or property or other rights important to you.

YOU SHOULD TAKE THIS PAPER TO YOUR LAWYER AT ONCE. IF YOU DO NOT HAVE A LAWYER OR CANNOT AFFORD ONE, GO TO OR TELEPHONE THE OFFICE SET FORTH BELOW TO FIND OUT WHERE YOU CAN GET LEGAL HELP.

Lackawanna County Bar Association
233 Penn Avenue
Scranton, PA 18503
Telephone: (570) 969-9161

AVISO

Le han demandado a usted en la corte. Si usted quiere defenderse de estas demandas expuestas en las paginas siguientes, usted tiene veinte (20) dias de plazo al partir de la fecha de la demanda y la notificacion. Hace falta asentar una comparesencia escrita o en persona o con un abogado y entregar a la corte en forma escrita sus defensas o sus objeciones a las demandas en contra de su persona. Sea avisado que si usted no se defiende, la corte tomara medidas y puede continuar la demanda en contra suya sin previo aviso o notificacion. Ademas, la corte puede decidir a favor del demandante y requier que usted cumpla con todas las provisiones de esta demanda. Usted puede perder dinero o sus propiedades u otros derechos importantes para usted.

LLEVE ESTA DEMANDA A UN ABOGADO INMEDIATAMENTE, SI NO TIENE ABOGADO O SI NO TIENE EL DINERO SUFICIENTE DE PAGAR TAL SERVICIO, VAYA EN PERSONA O LLAME POR TELEFONO A LA OFICINA CUYA DIRECCION SE ENCUENTRA ESCRITA ABAJO PARA AVERIGUAR DONDE SE PUEDE CONSEGUIR ASISTENCIA LEGAL.

Lackawanna County Bar Association
233 Penn Avenue
Scranton, PA 18503
Telefono: ((570) 969-9161

JANE DOE INDIVIDUALLY AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED, Plaintiff, v. GEISINGER HEALTH and DOE ENTITIES 1-99, Defendants.	IN THE COURT OF COMMON PLEAS OF LACKAWANNA COUNTY, PENNSYLVANIA CIVIL ACTION - LAW Case No. 23cv1911 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Jane Doe ("Plaintiff"), individually and on behalf of all other current Citizens of the Commonwealth of Pennsylvania similarly situated ("Class Members"), brings suit against Defendants Geisinger Health and Doe Entities 1-99 (collectively "Defendants" or "Geisinger"), and upon personal knowledge as to Plaintiff's own conduct and on information and belief as to all other matters based upon investigation by counsel, allege as follows:

NATURE OF ACTION AND ALLEGATIONS

1. This case arises from Geisinger's systematic violation of the medical privacy rights of its patients, exposing highly sensitive personal information to third parties without those patients' knowledge or consent.

2. Geisinger assures visitors to its website that "Geisinger is committed to protecting the privacy and confidentiality of its patients' and members' medical information."[1] Contrary to these assurances, however, Geisinger does not follow these policies, nor the law prohibiting such disclosures.

3. As recently as July 7, 2022, Geisinger disclosed information about its patients—including their status as patients, their physicians, their medical treatments, the hospitals they visited, and their personal identities—to Facebook. As of the filing of this complaint, Geisinger continues to disclose the same kinds of information to Google and other third parties without its patients' knowledge, authorization, or consent.

4. Geisinger discloses this personal health information through the deployment of various digital marketing and automatic rerouting tools embedded on its websites that purposefully and intentionally discloses patients' personal health information to third parties who exploit that information for advertising purposes. Geisinger's use of these tools causes its patients' personally identifiable information and the contents of its patients' communications exchanged with Geisinger to be automatically redirected to third parties in violation of those patients' reasonable expectations of privacy, their rights as patients, their rights as citizens of Pennsylvania, and both the express and implied promises of Geisinger.

[1] https://www.geisinger.org/about-geisinger/corporate/corporate-policies/hipaa

5. Geisinger's conduct in disclosing such protected health information about its patients to Facebook and other third parties violates Pennsylvania law, including, but not limited to, 18 Pa. C.S. §§5701 *et seq* (the Wiretapping and Electronic Surveillance Control Act), 28 Pa. Code § 115.27 (Confidentiality of Medical Records), 49 Pa. Code § 16.61(a)(1) (Unprofessional and Immoral Conduct), and the duty of physician-patient confidentiality recognized in *Haddad v. Gopal*, 787 A.2d 975, 980 (Pa. Super. 2001).

6. On behalf of herself and all similarly situated citizens in the Commonwealth of Pennsylvania, Plaintiff seeks an order enjoining Geisinger from further unauthorized disclosures of their personal information; awarding statutory damages in the amount of $1,000 per violation, attorney's fees and costs; and granting any other preliminary or equitable relief the Court deems appropriate.

PARTIES TO THE ACTION

7. Defendant Geisinger Health is a Pennsylvania corporation with a registered address of 100 N. Academy Avenue, Danville, PA 17821. Defendant owns and operates multiple hospitals and medical clinics in Pennsylvania, including Geisinger Medical Center, Geisinger Community Medical Center, Geisinger Wyoming Valley Medical Center, Geisinger Medical Center Muncy, Geisinger Bloomsburg Hospital, Geisinger Lewistown Hospital, Geisinger Shamokin Area Community Hospital, Geisinger South Wilkes-Barre, Geisinger St. Luke's Hospital, and Geisinger Jersey Shore, serving more than 600,000 patients. Defendant also owns and operates the website and patient portal found at https://www.geisinger.org/.

8. Defendants Doe Entities 1-99 are, upon information and belief, Pennsylvania entities operating in conjunction with the other Defendants and engaged in the same unlawful conduct described herein.

9. The Defendants listed above collectively do business throughout the Commonwealth of Pennsylvania as "Geisinger." Defendants are jointly engaged in a commercial enterprise with a common economic purpose, and the violations outlined herein were in furtherance of that common economic purpose.

10. Plaintiff Jane Doe is a Pennsylvania citizen residing in Lackawanna County, Pennsylvania who has been a Geisinger patient and has utilized its website. Plaintiff Jane Doe can be served at 1524 Locust Street, Philadelphia, PA 19102.

JURISDICTION AND VENUE

11. This Court has personal jurisdiction over Geisinger pursuant to 42 Pa. C.S.A. §§ 5301, 5308, & 5322 because the Geisinger Defendants regularly conduct continuous and systematic business throughout the Commonwealth of Pennsylvania, have engaged in acts that have caused harm in this Commonwealth, have violated the statutes of this Commonwealth, and/or are formed under the laws of this Commonwealth.

12. Venue is appropriate in Lackawanna County pursuant to Pa R.C.P. 1006, 2130, 2156, and 2179 because the Geisinger Defendants' principal place of business is in Lackawanna County, they regularly conduct business there, and, upon information and belief, many of the acts or conduct giving rise to the cause of action asserted herein took place in Lackawanna County. Venue is also appropriate in this Court because Plaintiff Jane Doe resides in Lackawanna County and Geisinger has caused harm Plaintiff harm in Lackawanna County.

FACTUAL BACKGROUND

A. Geisinger routinely disclosed the protected health information of its patients to third parties including Facebook.

13. Plaintiff Jane Doe is a patient of Geisinger who has received treatment from Geisinger's hospital facilities, including Geisinger Community Health Medical Center in Scranton, Pennsylvania.

14. Pennsylvania courts have long recognized a "right to privacy" in the Constitution of the Commonwealth.[2] The Pennsylvania Supreme Court, in fact, has held that the Pennsylvania Constitution "provides even more rigorous and explicit protections for a person's right to privacy than does the United States Constitution."[3]

15. Medical patients in Pennsylvania such as Jane Doe have a legal interest in preserving the confidentiality of their communications with healthcare providers and have reasonable expectations of privacy that their personally identifiable information and communications will not be disclosed to third parties by Geisinger without their express written consent and authorization.[4]

16. As a health care provider, Geisinger has fiduciary, common law, and statutory duties to keep patient data, communications, diagnoses, and treatment information completely confidential unless authorized to make disclosures by the patient.

---

[2] *See, e.g., Pennsylvania State Educ. Ass'n v. Commonwealth Dep't of Cmty. & Econ. Dev.*, 637 Pa. 337, 340, 148 A.3d 142, 144 (2016)

[3] *See id.* at 352-353 (internal quotations omitted).

[4] *See, e.g., In re T.R.*, 557 Pa. 99, 105, 731 A.2d 1276, 1279 (1999) (recognizing constitutional "right to privacy" protects a citizen's interest in "avoiding disclosure of personal matters."); *In re "B"*, 482 Pa. 471, 486, 394 A.2d 419, 426 (1978) (barring disclosure of a patient's "psychiatric records" under the constitutional right to privacy.)

17. Patients are aware of (and must be able to reply upon) the protections, obligations, and expectations provided by statutory, regulatory, and common law as well as the promises of confidentiality contained within the Hippocratic Oath.

18. Geisinger expressly and impliedly promises patients that they will maintain and protect the confidentiality of personally identifiable patient information and communications.

19. Patients rely on these promises, obligations, and protections when seeking medical care.

20. Patients also have reasonable expectations of privacy that their personally identifiable information and communications will not be disclosed to third parties by Geisinger without their express written consent and authorization.

21. Geisinger operates the website https://www.geisinger.org/ for patients.

22. Geisinger's website is designed for interactive communication with patients, including scheduling appointments, searching for physicians, paying bills, requesting medical records, learning about medical issues and treatment options, and joining support groups.

23. Geisinger encourages patients to use digital tools on its website to seek and receive health services. The home page of Geisinger's website is designed for use by patients, and provides patients with tools to seek treatment, such as buttons that patients can click to find a doctor, research treatments, and learn about Geisinger's services.

24. Geisinger also maintains a patient portal, which allows patients to make appointments, access medical records, view lab results, and exchange communications with their health care providers.

25. Notwithstanding patients' reasonable expectations of privacy, Geisinger's legal duties of confidentiality, and Geisinger's express promises to the contrary, Geisinger disclosed the

contents of patients' communications and protected healthcare information via automatic re-routing mechanisms embedded in the websites operated by Geisinger without patients' knowledge, authorization, or consent. In doing so, Geisinger systematically violated the medical privacy rights of its patients by causing the unauthorized disclosure of patient communications to be transmitted to Facebook, Google, and other third-party marketing companies.

26. While Geisinger intentionally incorporated tracking technologies into its website, Geisinger never disclosed to Plaintiff or Class Members that it shared their sensitive and confidential communications with Facebook, Google, and others. As a result, Plaintiff and Class Members were unaware that their private information was being surreptitiously transmitted to third parties when they visited Geisinger's website.

27. By design, none of the tracking mechanisms employed by Geisinger are visible to patients visiting Geisinger's website.

28. Geisinger did not warn or otherwise disclose to Plaintiff and Class Members that Geisinger bartered their confidential medical communications to Facebook, Google, and other third parties for marketing purposes.

29. Plaintiff and Class Members never consented, agreed, or otherwise authorized Geisinger to disclose their confidential medical communications, particularly not beyond the limits of Geisinger's express promises to protect the confidentiality of Plaintiff's and Class Members' private information.

30. Upon information and belief, Geisinger intercepted and disclosed the following non-public private information to Facebook:

a. Plaintiff's and Class Members' status as patients;

b. Plaintiff's and Class Members' communications with Geisinger via its website;

c. Plaintiff's and Class Members' use of Geisinger's patient portal;

d. Plaintiff's and Class Members' searches for information regarding specific medical conditions and treatments, their medical providers, and their physical location.

31. Geisinger interfered with Plaintiff's and Class Members' privacy rights when it implemented technology (including the Meta Pixel) that surreptitiously tracked, recorded, and disclosed Plaintiff's and Class Members' confidential information to Facebook, Google, and other third parties.

32. Geisinger also breached its obligations to Plaintiff and Class Members in multiple other ways, including (1) failing to obtain their consent to disclose their private information to Facebook and other third parties, (2) failing to adequately review its marketing programs and web-based technology to ensure its website was safe and secure, (3) failing to remove or disengage software code that was known and designed to share patients' private information with third parties, (4) failing to take steps to block the transmission of Plaintiff's and Class Members' private information to Facebook and other third-party advertising companies, (5) failing to warn Plaintiff and Class Members that Geisinger was routinely bartering their private information to Facebook via the Meta Pixel, and (6) otherwise ignoring Geisinger's common and statutory obligations to protect the confidentiality of patient's protected health information.

33. Plaintiff and Class Members have suffered injury because of Geisinger's conduct. Their injuries include invasion of privacy and the continued and ongoing risk of irreparable harm from the disclosure of their most sensitive and personal information.

B. The nature of Geisinger's unauthorized disclosure of patients' health care information.

34. Geisinger's disclosures of patients' personal healthcare information occurred because Geisinger intentionally deployed source code on the websites it operates, including

https://www.geisinger.org/, that cause patients' personally identifiable information (as well as the exact contents of their communications) to be transmitted to third parties.

35. By design, these third parties receive and record the exact contents of patient communications before the full response from Geisinger to patients has been rendered on the screen of the patient's computer device and while the communication between Geisinger and the patient remains ongoing.

36. For example, when Plaintiff or a Class Member accessed Geisinger's website pages hosting the Meta Pixel, the Meta Pixel software directed their browsers to send a message to Facebook's servers. The information that Geisinger sent to Facebook included the private information that Plaintiff and Class Members communicated to Geisinger's website, such as the type of medical appointment the patient made, the date, and the specific doctor the patient was seeing. Such private information allows third-party advertising companies like Facebook to determine that a specific patient was seeking a specific type of confidential medical treatment. This kind of disclosure also allows Facebook to reasonably infer that a specific patient was being treated for specific types of medical conditions, such as cancer and pregnancy.

37. Such private information allows third-party advertising companies like Facebook to determine that a specific patient was seeking a specific type of confidential medical treatment. This kind of disclosure also allows Facebook to reasonably infer that a specific patient was being treated for specific types of medical conditions, such as cancer.

38. Websites like those maintained by Geisinger are hosted by a computer server through which the business in charge of the website exchanges and communicates with internet users via their web browsers.

39. Every website is hosted by a computer server through which the entity in charge of the website exchanges communications with internet users via a client device, such as a computer, tablet, or smart phone, via the client device's web browser.

40. Web browsers are software applications that allow users to exchange electronic communications over the internet.

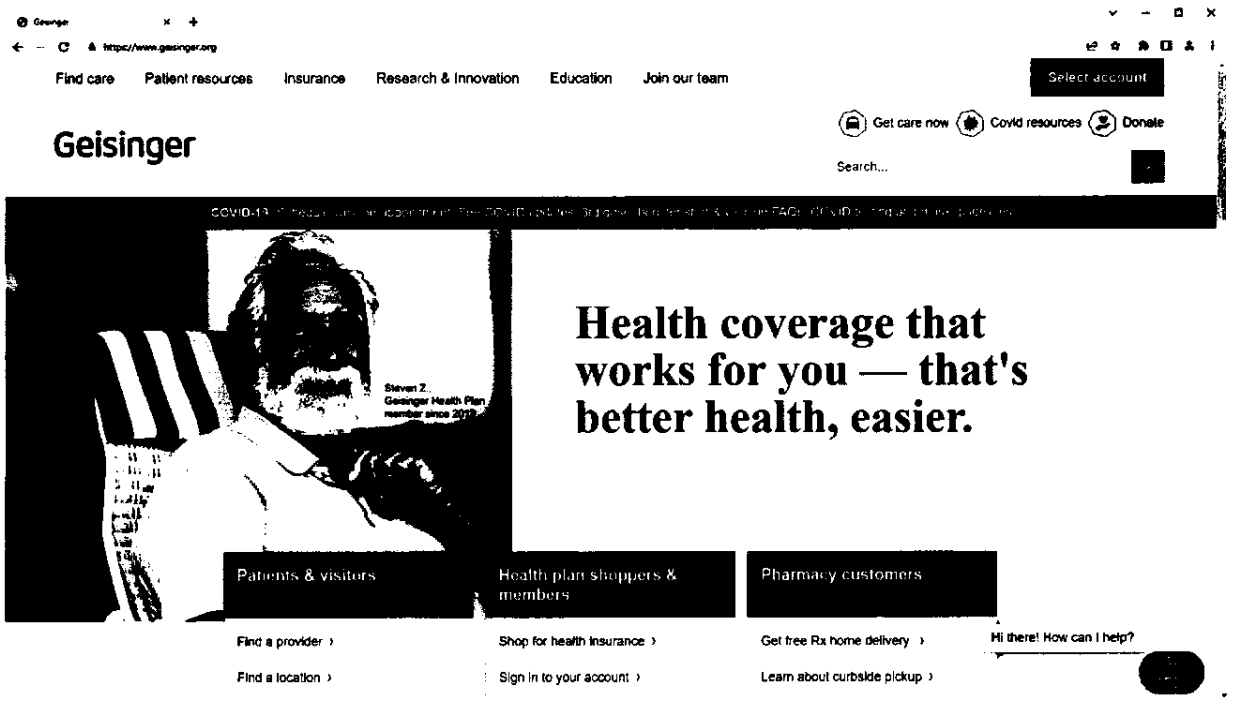
41. Each exchange of an electronic communication over the internet typically consists of an HTTP request from a client device and an HTTP response from a server. When a user types a URL into a web browser, for example, the URL is sent as an HTTP request to the server corresponding to the web address, and the server then returns an HTTP response that consists of a web page to render in the client device's web browser.

42. In addition to specifying the URL, HTTP requests can also send data to the host server, including users' cookies. Cookies are text files stored on client devices to record data, often containing sensitive, personally identifiable information.

43. In turn, HTTP responses may consist, among other things, of a web page, another kind of file, text information, or error codes.

44. A web page consists primarily of "Markup" and "Source Code." The markup of a web page comprises the visible portion of that web page. Markup is displayed by a web browser in the form of words, paragraphs, images, and videos displayed on a users' device screen. The source code of a web page is a set of instructions that commands the browser to take certain actions, either when the web page loads or when a specified event triggers the code.

45. For example, typing https://www.geisinger.org/ into a browser sends an HTTP request to Geisinger's website, which returns a HTTP response in the form of the home page of Geisinger's website:



46. Source code is not visible on the client device's screen, but it may change the markup of a webpage, thereby changing what is displayed on the client device's screen. Source code may also execute a host of other programmatic instructions, including commanding a web browser to send data transmissions in the form of HTTP requests to the website's server, or, as is the case with Geisinger's website, to third parties via pixels.

47. For example, Geisinger's website includes software code that transmits HTTP requests *directly* to Facebook, including patients' private health information, every time a patient interacts with a page on its website.

48. The basic command that web browsers use to exchange data and user communications is called a GET request.[5] For example, when a patient types "heart failure treatment" into the search box on Geisinger's website and hits 'Enter,' the patient's web browser

[5] https://www.w3schools.com/tags/ref_httpmethods.asp

makes a connection with the server for Geisinger's website and sends the following request: "GET search/q=heart+failure+treatment."

49. When a server receives a GET request, the information becomes appended to the next URL (or "Uniform Resource Locator") accessed by the user. For example, if a user enters "respiratory problems" into the query box of a website search engine, and the search engine transmits this information using a GET request method, then the words "respiratory" and "problems" will be appended to the query string at the end of the URL of the webpage showing the search results.

50. The other basic transmission command utilized by web browsers is POST, which is typically employed when a user enters data into a form on a website and clicks 'Enter' or some other form of submission button. POST sends the data entered in the form to the server hosting the website that the user is visiting.

51. In response to receiving a GET or POST request, the server for the entity with which the user is exchanging communications, in this case Geisinger's server, will send a set of instructions to the web-browser, commanding the browser with source code that (1) directs the browser on how to render the entity's response and, in many circumstances, (2) commands the browser to transmit personally identifiable data about the Internet user and re-direct the precise content of the user's GET or POST requests to various third parties.

52. In addition to these communications between Geisinger and the patient, however, when a patient communicates with Geisinger's website (whether by typing in a webpage, putting in a search, clicking on a hyperlink, logging into the Geisinger patient portal, maneuvering through the patient portal, or otherwise), Geisinger also causes some of that information to be transmitted to third parties without the patient's knowledge or authorization. The third parties to whom user

data is transmitted and the content of communications redirected are typically procured by websites to track users' personally identifiable data and communications for marketing purposes—i.e., targeted advertising.

53. In many such cases, the third parties acquire the content of user communications through a 1x1 pixel (the smallest dot on a user's screen) called a web bug, tracking pixel, or web beacon. These web-bugs are tiny and purposefully camouflaged to remain invisible to the user.

54. Web bugs can be placed directly on a page by a web developer or can be funneled through a "tag manager" service to make the invisible tracking run more efficiently and to further obscure the third parties to whom the website transmits personally identifiable user data and re-directs the content of communications.

55. On information and belief, Geisinger deploys Google Tag Manager on its websites through an "iframe," a nested "frame" that exists within the Geisinger web properties, including inside Geisinger's patient portal, that is, in reality, an invisible window through which Geisinger funnels web bugs for third parties to secretly acquire the content of patient communications without any knowledge, consent, authorization, or further action of patients.

56. By design, none of the tracking is visible to patients who visit Geisinger's web properties.

57. Once the initial connection is made between a user and a website, the communications commence and continue between the parties in a bilateral fashion until the user leaves the website.

58. Unbeknownst to users, however, the website's server may also transmit the user's communications to third parties via third party tracking tools. Indeed, Google warns website

developers and publishers that installing its ad tracking software on webpages employing GET requests will result in users' personally identifiable information being disclosed to Google.[6]

59. Third parties (such as Facebook and Google) use the information they receive to track user data and communications for marketing purposes.

60. In many cases, third-party marketing companies acquire the content of user communications through a 1x1 pixel (the smallest dot on a user's screen) called a tracking pixel, a web-bug, or a web beacon. These tracking pixels are tiny and are purposefully camouflaged to remain invisible to users.

61. Tracking pixels can be placed directly on a web page by a developer, or they can be funneled through a "tag manager" service to make the invisible tracking run more efficiently and to further obscure the third parties to whom users' personally identifiable data and communications are transmitted without their knowledge or consent.

62. Tag managers are simple enough that non-programmers can use them to deploy and remove digital tracking tools from web-properties with just the click of a few buttons.

63. Geisinger deploys Google Tag Manager on its website through an "iframe," a nested "frame" that exists within the Geisinger's website that is, in reality, an invisible window through which Geisinger funnels tracking pixels for third parties to secretly acquire the content of patient communications without any knowledge, consent, authorization, or further action of patients.

64. Geisinger's Google Tag Manager source code is designed to be invisible. The source code employed by Geisinger specifies an "iframe" with a height of 0, width of 0, display of none, and visibility hidden.

[6] https://support.google.com/platformspolicy/answer/6156630?hl=en

65. Geisinger then funnels invisible 1x1 tracking pixels or web-bugs through this purposely invisible iframe to help third parties track, acquire, and record patient data and communications.

66. By design, none of the tracking is visible to patients visiting Geisinger's website.

67. These tracking pixels can collect dozens of data points about individual website users who interact with a website. For example, when a patient clicks through Geisinger's website to the page describing Geisinger's "Neurology" services at https://www.geisinger.org/patient-care/conditions-treatments-specialty/neurology, the source code deployed on Geisinger's website causes personally identifiable data and the content of patient communications to be transmitted to third parties:

68. By design, the transmission of patient data to third parties occurs before Geisinger's responsive communications about "Neurology" have been delivered in full to the patient.

69. In addition to Google Tag Manager, other source code is also placed on Geisinger's website, resulting in the interception and transmission of patient personal health information to multiple third parties.

70. A web site developer who chooses to deploy third-party source code, like a tracking pixel, on their website must enter the third-party source code directly onto their website for every third party they wish to send user data and communications. This source code operates invisibly in the background when users visit a site employing such code.

71. For example, one of the world's most prevalent tracking pixels, called the Meta Pixel, is provided by Facebook. Tracking pixels such as the Meta Pixel tool allow Geisinger and Facebook to secretly track, intercept, record, and transmit every patient communication made on Geisinger's website. When patients visit Geisinger's website, unbeknownst to them, the web page displayed on the patient's browser includes the Meta Pixel as embedded code, which is not visible to patients or other visitors to Geisinger's website. This code is triggered when a patient or visitor interacts with the web page. Each time the Meta Pixel is triggered, the software code is executed and sends patient's private information directly to Facebook.

72. The Meta Pixel and similar tracking pixels act like a physical wiretap on a phone. Like a physical wiretap, pixels do not appear to alter the function of the communication device on which they surreptitiously installed. Instead, these pixels like in wait until they are triggered by an event, at which time they effectively open a channel through the website funnels data about users and their actions to third parties via a hidden HTTP request that is never shown to or agreed to by the user.

73. For example, a patient can trigger an HTTP request by interacting with the search bar on Geisinger's website by typing a term such as "breast cancer" into the search bar and then

hitting enter. Geisinger's server in turn sends an HTTP response, which results in the search results being displayed.

74. This is not the only HTTP request, however, that is created by a patient's interaction with Geisinger's website. In fact, at the very same time the web page is instructed to send an HTTP request to Geisinger requesting search results, the embedded Meta Pixel, acting as a tap, is triggered, such that Geisinger's website is also instructed to send an HTTP request directly to Facebook and Google, informing them of the patient's exact search and the patient's personally identifiable information.

C. Tracking pixels provide third parties with a trove of personally identifiable information.

75. Tracking pixels are especially pernicious because they result in the disclosure of a variety of personally identifiable information.

76. For example, an IP address is a numerical identifier that identifies each computer connected to the internet. IP addresses are used to identify and route communications on the internet. IP addresses of individual users are used by internet service providers, websites, and tracking companies to facilitate and track internet communications and content. IP addresses also offer advertising companies like Facebook a unique and semi-persistent identifier across devices—one that has limited privacy controls.[7]

77. Because of their uniquely identifying characteristics, IP addresses are considered personally identifiable information ("PII"). 45 CFR § 164.514. Tracking pixels can (and typically do) collect website visitors' IP addresses.

78. Whenever a Geisinger patient uses the Geisinger web properties, Geisinger uses and causes the disclosure of the patient's IP addresses to third parties with each re-directed

[7] https://adtechexplained.com/the-future-of-ip-address-as-an-advertising-identifier/

communication described herein, including patient communications about providers, conditions, treatments, appointments, bills, registration, and log-ins to the patient portal.

79. Likewise, internet cookies are also protected personally identifiable information. 45 CFR § 164.514(b)(2)(i)(H), (J), (M), (N), and (R).

80. In the early years of the internet, advertising on websites followed the same model as traditional newspapers. Just as a sporting goods store would choose to advertise in the sports section of a traditional newspaper, advertisers on the early internet paid for ads to be placed on specific web pages based on the type of content displayed.

81. Computer programmers eventually developed 'cookies'—small text files that web servers can place on a user's browser and computer when a user's browser interacts with a website server. Eventually some cookies were designed to acquire and record an individual internet user's communications and activities on websites across the internet.

82. Cookies are designed to operate as a means of identification for internet users. Advertising companies like Facebook and Google have developed methods for monetizing and profiting from cookies. These companies use third-party tracking cookies to help them acquire and record user data and communications in order to sell targeted advertising that is customized to a user's personal communications and browsing history. To build individual profiles of internet users, third party advertising companies assign each user a unique (or a set of unique) identifiers to each user.

83. Cookies are considered personally identifiable information, and tracking pixels can collect cookies from website visitors.

84. In general, cookies are categorized by (1) duration and (2) party.

85. There are two types of cookies classified by duration.

86. "Session cookies" are placed on a user's computing device only while the user is navigating the website that placed and accesses the cookie. The user's web browser typically deletes session cookies when the user closes the browser.

87. "Persistent cookies" are designed to survive beyond a single internet-browsing session. The party creating the persistent cookie determines its lifespan. As a result, a persistent cookie can acquire and record a user's internet communications for years and over dozens or even hundreds of websites. Persistent cookies are also called "tracking cookies."

88. Cookies are also classified by the party that uses the collected data.

89. "First-party cookies" are set on a user's device by the website with which the user is exchanging communications. First-party cookies can be helpful to the user, server, and/or website to assist with security, login, and functionality.

90. "Third-party cookies" are set on a user's device by website servers other than the website or server with which the user is exchanging communications. For example, the same patient who visits Geisinger's website will also have cookies on their device from third parties, such as Facebook and Google. Unlike first-party cookies, third-party cookies are not typically helpful to the user. Instead, third-party cookies are typically used for data collection, behavioral profiling, and targeted advertising.

91. Data companies like Facebook have developed methods for monetizing and profiting from cookies. These companies use third-party tracking cookies to help them acquire and record user data and communications in order to sell advertising that is customized to a user's communications and habits. To build individual profiles of internet users, third party data companies assign each user a unique identifier or set of unique identifiers.

92. Traditionally, first-party and third-party cookies were kept separate. An internet security policy known as the same-origin policy required web browsers to prevent one web server from accessing the cookies of a separate web server. For example, although Geisinger can deploy source code that uses Facebook third-party cookies to help Facebook acquire and record a patient's communications, Geisinger is not permitted direct access to Facebook third-party cookie values. The reverse *was* also true: Facebook was not provided direct access to the values associated with first-party cookies set by companies like Geisinger. But Big Data companies have designed a way to hack around the same-origin policy so that third-party data companies like Facebook can gain access to first-party cookies.

93. JavaScript source code developed by third party data companies and placed on a webpage by a developer such as Geisinger can bypass the same-origin policy to send a first-party cookie value in a tracking pixel to the third-party data company. This technique is known as "cookie syncing," and it allows two cooperating websites to learn each other's cookie identification numbers for the same user. Once the cookie syncing operation is completed, the two websites can exchange any information that they have collected and recorded about a user that is associated with a cookie identifier number. The technique can also be used to track an individual who has chosen to deploy third-party cookie blockers.

94. In effect, cookie syncing is a method through which Facebook, Google, and other third-party marketing companies set and access third-party cookies that masquerade as first-party cookies. By designing these special third-party cookies that are set for first-party websites, Facebook and Google hack their way around any cookie blockers that users set up to stop their tracking. On information and belief, the letters fbp are an acronym for Facebook Pixel.

95. The Facebook _fbp cookie is a Facebook identifier that is set by Facebook source code and associated with the health care provider using the Meta Pixel. The _fbp cookie is used as a unique identifier for patients by Facebook.

96. The _fbp cookie is also a third-party cookie in that it is also a cookie associated with Facebook that is used by Facebook to associate information about a person and their communications with non-Facebook entities while the person is on a non-Facebook website or app.

97. When Plaintiff and Class Members visited Geisinger's web properties, source code that Geisinger installed on its website—without any action or authorization by Plaintiff and Class Members—surreptitiously installed cookies such as the _fbp, _ga, and _gid cookies onto Plaintiff's and Class members' computing devices. These are cookies associated with the third-parties like Facebook and Google but which Geisinger deposits on Plaintiff's and Class members' computing devices by disguising them as first-party cookies.

98. Geisinger engages in cookie syncing with Facebook, Google, and other third parties.

99. Whenever a Geisinger patient uses the Geisinger website, Geisinger uses and causes the disclosure of patient cookie identifiers with each re-directed communication, including patient communications about providers, conditions, treatments, appointments, bills, registration, and log-ins to the Geisinger patient portal.

100. Geisinger's cookie disclosures include the deployment of cookie syncing techniques that cause the disclosure of first-party cookie values that Geisinger assigns to patients to be made to third parties.

101. On information and belief, Geisinger requires patients using its patient portal to have enabled first-party cookies to gain access to its patient portal.

102. If a patient takes an action to delete or clear third-party cookies from their device, the _fbp cookie is not impacted—even though it is a Facebook cookie—because Facebook has disguised it as a first-party cookie. Facebook also uses IP addresses and user-agent information to match the health information it receives from Geisinger with Facebook users.

103. Geisinger engages in cookie syncing with Facebook, Google, and other third parties.

104. Geisinger's cookie disclosures include the deployment of cookie syncing techniques that cause the disclosure of the first-party cookie values that Geisinger assigns to patients to also be made to third parties.

105. Geisinger uses and causes the disclosure of patient cookie identifiers with each re-directed communication described herein, including patient communications concerning individual providers, conditions, and treatments.

106. A third type of personally identifiable information is what data companies refer to as a "browser-fingerprint." A browser-fingerprint is information collected about a computing device that can be used to identify the specific device.

107. A browser-fingerprint can be used to identify a device when the device's IP address is hidden, and cookies are blocked.

108. The Electronic Frontier Foundation has explained:

> When a site you visit uses browser fingerprinting, it can learn enough information about your browser to uniquely distinguish you from all the other visitors to that site. Browser fingerprinting can be used to track users just as cookies do, but using much more subtle

> and hard-to-control techniques. In a paper EFF released in 2010, we found that a majority of users' browsers were uniquely identifiable given existing fingerprinting techniques. Those techniques have only gotten more complex and obscure in the intervening years. By using browser fingerprinting to piece together information about your browser and your actions online, trackers can covertly identify users over time, track them across websites, and building an advertising profile of them.[8]

109. These browser-fingerprints can be used to uniquely identify individual users when a computing device's IP address is hidden or cookies are blocked and can provide a wide variety of data. As Google has explained, "With fingerprinting, developers have found ways to use tiny bits of information that vary between users, such as what device they have or what fonts they have installed to generate a unique identifier which can then be used to match a user across websites."[9] The value of browser-fingerprinting to advertisers (and trackers who want to monetize aggregated data) is that they can be used to track website users just as cookies do, but it employs much more subtle techniques.[10] Additionally, unlike cookies, users cannot clear their fingerprint and therefore cannot control how their personal information is collected.[11]

110. In 2017, researchers demonstrated that browser fingerprinting techniques can successfully identify 99.24 percent of all users.[12]

111. Browser-fingerprints are also considered personal identifiers, and tracking pixels can collect browser-fingerprints from website visitors. Browser-fingerprints are protected personal identifiers under HIPAA. *See* 45 C.F.R. § 164.514(b)(2)(i)(M), (R).

---

[8] Katarzyna Szymielewicz and Bill Dudington, *The GDPR and Browser Fingerprinting: How It Changes the Game for the Sneakiest Web Trackers*, Electronic Frontier Foundation (June 19, 2018) (available at https://www.eff.org/deeplinks/2018/06/gdpr-and-browser-fingerprinting-how-it-changes-game-sneakiest-web-trackers).

[9] https://www.blog.google/products/chrome/building-a-more-private-web/

[10] https://pixelprivacy.com/resources/browser-fingerprinting/

[11] https://www.blog.google/products/chrome/building-a-more-private-web/

[12] https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/cross-browser-fingerprinting-os-and-hardware-level-features/

112. Whenever a Geisinger patient such as Plaintiff uses Geisinger's web properties, Geisinger uses and causes the disclosure of data sufficient for third parties to create a browser-fingerprint identifier with each re-directed communication described herein, including patient communications concerning individual providers, conditions, and treatments.

113. Geisinger uses and causes the disclosure of data sufficient for third parties to create a browser-fingerprint identifier with each re-directed communication described herein, including patient communications concerning individual providers, conditions, and treatments.

114. A fourth kind of personally identifiable information protected by law against disclosure are unique user identifiers (such as Facebook's "Facebook ID") that permit companies like Facebook to quickly and automatically identify the personal identity of its user across the internet whenever the identifier is encountered. A Facebook ID is an identifiable number string that is connected to a user's Facebook profile. Anyone with access to a user's Facebook ID can locate a user's Facebook profile.

115. Unique personally identifiable information such as a person's Facebook ID are likewise capable of collection through pixel trackers.

116. Each of the individual data elements described above is personally identifiable on their own. However, Geisinger's disclosures of such personally identifiable data elements do not occur in a vacuum. The disclosures of the different data elements are tied together and, when taken together, these data elements are even more accurate in identifying individual patients, particularly when disclosed to data companies such as Facebook, Google, and other internet marketing companies that expressly state that they use such data elements to identify individuals.

D. Facebook's Business Model: Exploiting Users' Personal Data to Sell Advertising.

117. Facebook, a social media platform founded in 2004 and today operated by Meta

Platforms, Inc., was originally designed as a social networking website for college students.

118. Facebook describes itself as a "real identity" platform.[13] This means that users are permitted only one account and must share "the name they go by in everyday life." To that end, Facebook requires users to provide their first and last name, along with their birthday, telephone number and/or email address, and gender, when creating an account.

119. In 2007, realizing the value of having direct access to millions of consumers, Facebook began monetizing its platform by launching "Facebook Ads," proclaiming this service to be a "completely new way of advertising online," that would allow "advertisers to deliver more tailored and relevant ads." Facebook has since evolved into one of the largest advertising companies in the world. Facebook can target users so effectively because it surveils user activity both on and off its website through the use of tracking pixels. This allows Facebook to make inferences about users based on their interests, behavior, and connections.

120. Today, Facebook provides advertising on its own social media platforms, as well as other websites through its Facebook Audience Network. Facebook has more than 2.9 billion users.[14]

121. Facebook maintains profiles on users that include users' real names, locations, email addresses, friends, likes, and communications. These profiles are associated with personal identifiers, including IP addresses, cookies, and other device identifiers. Facebook also tracks non-users across the web through its internet marketing products and source code. Facebook employs algorithms, powered by machine learning tools, to determine what advertisements to show users based on their habits and interests, and utilizes tracking software such as the Meta Pixel

[13] https://www.wsj.com/articles/how-many-users-does-facebook-have-the-company-struggles-to-figure-it-out-11634846701#:~:text=Facebook%20said%20in%20its%20most,of%20them%20than%20developed%20ones.
[14] https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

to monitor and exploit users' habits and interests.

122. Tracking information about users' habits and interests is a critical component of Facebook's business model because it is precisely this kind of information that allows Facebook to sell advertising to its customers. Facebook uses plug-ins and cookies to track users' browsing histories when they visit third-party websites. Facebook then compiles these browsing histories into personal profiles which are sold to advertisers to generate profits.

123. Facebook offers several advertising options based on the type of audience that an advertiser wants to target. Those options include targeting "Core Audiences," "Custom Audiences," "Look Alike Audiences," and even more granulated approaches within audiences called "Detailed Targeting." Each of Facebook's advertising tools allow an advertiser to target users based, among other things, on their personal data, including geographic location, demographics (e.g., age, gender, education, job title, etc.), interests, (e.g., preferred food, movies), connections (e.g., particular events or Facebook pages), and behaviors (e.g., purchases, device usage, and pages visited). This audience can be created by Facebook, the advertiser, or both working in conjunction.

124. Ad Targeting has been extremely successful due to Facebook's ability to target individuals at a granular level. For example, among many possible target audiences, "Facebook offers advertisers 1.5 million people 'whose activity on Facebook suggests that they're more likely to engage with/distribute liberal political content' and nearly seven million Facebook users who 'prefer high-value goods in Mexico.'"[15] Aided by highly granular data used to target specific users, Facebook's advertising segment quickly became Facebook's most successful business unit, with millions of companies and individuals utilizing Facebook's advertising services.

[15] https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html

E. Facebook's Meta Pixel tool allows Facebook to track the personal data of individuals across a broad range of third-party websites.

125. To power its advertising business, Facebook uses a variety of tracking tools to collect data about individuals, which it can then share with advertisers. These tools include software development kits incorporated into third-party applications, its "Like" and "Share" buttons (known as "social plug-ins"), and other methodologies, which it then uses to power its advertising business.

126. One of Facebook's most powerful tools is called the "Meta Pixel." Once a third-party like Geisinger installs the Meta Pixel on its website, by default it begins sending user information to Facebook automatically.[16]

127. The Meta Pixel is a snippet of code embedded on a third-party website that tracks users' activities as users navigate through a website. Once activated, the Meta Pixel "tracks the people and type of actions they take." Meta Pixel can track and log each page a user visits, what buttons they click, as well as specific information that users input into a website. The Meta Pixel code works by sending Facebook a detailed log of a user's interaction with a website such as clicking on a product or running a search via a query box. The Meta Pixel also captures information such as what content a user views on a website.[17] The analytics provided by the Meta Pixel tool allow website developers to improve "website operability" by giving developers insight into how customers use and interact with companies' websites.[18]

128. When a patient uses their healthcare provider's website or application where the Meta Pixel is present, the Meta Pixel transmits the content of their communications to

[16] https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector
[17] https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector
[18] https://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3

Facebook, including but not limited to (1) signing up for a patient portal, (2) signing-in and -out of a patient portal, (3) taking actions inside a patient portal, (4) making or scheduling appointments, (5) exchanging communications related to doctors, treatments, payment information, health insurance information, prescription drugs, prescriptions, side effects, conditions, diagnoses, prognoses, or symptoms of health conditions, (6) conduct a search on a Facebook partner website, and (7) other information that qualifies as personal health information under state and federal laws.

129. In many circumstances, Facebook also obtains information from health care providers that identify a Facebook user's status as a patient and other health information that is protected by state and federal law. This occurs through tools that Facebook encourages health care providers to use to upload customer (i.e., patient) lists for use in its advertising systems.

130. The information Meta Pixel captures and disclose to Facebook includes a referrer header (or "URL"), which includes significant information regarding the user's browsing history, including the identifiable information of the individual internet user and the web server, as well as the name of the web page and the search terms used to find it.[19] When users enter a URL address into their web browser using the 'http' web address format, or click hyperlinks embedded on a web page, they are actually telling their web browsers (the client) which resources to request and where to find them. Thus, the URL provides significant information regarding a user's browsing history, identifiable information for the individual internet user and the web server, as well as the name of the web page and the search terms that the user used to find it.

[19] *In re Facebook*, 956 F.3d at 596.

131. When someone visits a third-party website page that includes the Meta Pixel code, the Meta Pixel code is able to replicate and send the user data to Facebook through a separate (but simultaneous) channel in a manner that is undetectable by the user.[20] This information is disclosed to Facebook regardless of whether a user is logged into their Facebook account at the time.

132. The transmission is instantaneous—indeed Facebook often receives the information before the health care provider does.

133. The transmission is invisible.

134. The transmission is made without any affirmative action taken by the patient.

135. The transmission occurs without any notice to the patient that it is occurring.

136. Facebook collects the transmitted identifiable health information and uses "cookies" to match it to Facebook users, allowing Facebook to target ads to a person who, for example, has used a patient portal and has exchanged communications about a specific condition, such as cancer.

137. The information Meta Pixel captures and discloses to Facebook includes a referrer header (or "URL"), which includes significant information regarding the user's browsing history, including the identifiable information of the individual internet user and the web server, as well as the name of the web page and the search terms used to find it.[21] When users enter a URL address into their web browser using the 'http' web address format, or click hyperlinks embedded on a web page, they are actually telling their web browsers (the client) which resources to request and where to find them. Thus, the URL provides significant information regarding a user's browsing

[20] *See, e.g., In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589, 596 (9th Cir. 2020) (explaining functionality of Facebook software code on third-party websites).
[21] *In re Facebook*, 956 F.3d at 596.

history, including identifiable information for the individual internet user and the web server, as well as the name of the web page and the search terms that the user used to find it.

138. These search terms and the resulting URLs divulge a user's personal interests, queries, and habits on third-party websites operating outside of Facebook's own platform. In this manner, Facebook tracks users browsing histories on third-party websites, and compiles these browsing histories into personal profiles which are sold to advertisers to generate revenue.[22]

139. For example, if Meta Pixel is incorporated on a shopping website, it may log what searches a user performed, which items of clothing a user clicked on, whether they added an item to their cart, as well as what they purchased. Along with this data, Facebook also receives personally identifiable information such as IP addresses, Facebook IDs, user agent information, device identifiers, and other data. All this personally identifiable data is available to be included each time the Meta Pixel forwards a user's interactions with a third-party website to Facebook's servers. Once Facebook receives this information, Facebook processes it, analyzes it, and assimilates it into datasets like its Core Audiences and Custom Audiences. Facebook can then sell this information to companies who wish to display advertising for products similar to what the user looked at on the original shopping website.

140. These communications with Facebook happen silently, without users' knowledge or consent. By default, the transmission of information to Facebook's servers is invisible. Facebook's Meta Pixel allows third-party websites to capture and send personal information a user provides to match them with Facebook or Instagram profiles, even if they are not logged into Facebook at the time.[23]

141. In exchange for installing its Meta Pixel, Facebook provides website owners like

[22] *In re Facebook*, 956 F.3d at 596.
[23] https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector

Geisinger with analytics about the ads they've placed on Facebook and Instagram and tools to target people who have visited their website.[24] The Meta Pixel collects data on website visitors regardless of whether they have Facebook or Instagram accounts.[25]

142. Facebook can then share analytic metrics with the website host, while at the same time sharing the information it collects with third-party advertisers who can then target users based on the information collected and shared by Facebook.

143. Facebook touted Meta Pixel (which it originally called "Facebook Pixel") as "a new way to report and optimize for conversions, build audiences and get rich insights about how people use your website." According to Facebook, the Meta Pixel is an analytics tool that allows business to measure the effectiveness of their advertising by understanding the actions people take on their websites."[26]

144. Facebook warns web developers that its Pixel enables Facebook "to match your website visitors to their respective Facebook User accounts."

145. Facebook recommends that its Meta Pixel code be added to the base code on every website page (including the website's persistent header) to reduce the chance of browsers or code from blocking Pixel's execution and to ensure that visitors will be tracked.

146. Once Meta Pixel is installed on a business's website, the Meta Pixel tracks users as they navigate through the website and logs which pages are visited, which buttons are clicked, the specific information entered in forms (including personal information), as well as "optional values" set by the business website. Facebook builds user profiles on users that include the user's real name, address, location, email addresses, friends, likes, and communications that Facebook

[24] https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites
[25] https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector
[26] https://www.oviond.com/understanding-the-facebook-pixel

associates with personal identifiers, such as IP addresses and the Facebook ID. Meta Pixel tracks this data regardless of whether a user is logged into Facebook.

147. Facebook tracks non-Facebook users through its widespread internet marketing products and source code and Mark Zuckerberg has conceded that the company maintains "shadow profiles" on nonusers of Facebook.[27]

148. For Facebook, the Meta Pixel tool embedded on third-party websites acts as a conduit for information, sending the information it collects to Facebook through scripts running in a user's internet browser, similar to how a "bug" or wiretap can capture audio information. The information is sent in data packets, which include personally identifiable data.

149. For example, the Meta Pixel is configured to automatically collect "HTTP Headers" and "Pixel-specific data." HTTP headers collect data including "IP addresses, information about the web browser, page location, document, referrer and person using the website." Pixel-specific data includes such data as the "Pixel ID and the Facebook Cookie."

150. Meta Pixel takes the information it harvests and sends it to Facebook with personally identifiable information, such as a user's IP address, name, email, phone number, and specific Facebook ID. Anyone who has access to this Facebook ID can use this identifier to quickly and easily locate, access, and view a user's corresponding Facebook profile. Facebook stores this information on its servers, and, in some instances, maintains this information for years.[28]

151. Facebook has a number of ways to gather personally identifiable information from individuals whose data is being forwarded from third-party websites through the Meta Pixel.

152. If a user has a Facebook account, the user data collected is linked to the individual

[27] https://techcrunch.com/2018/04/11/facebook-shadow-profiles-hearing-lujan-zuckerberg/
[28] https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites

user's Facebook account. For example, if the user is logged into their Facebook account when the user visits a third-party website where the Meta Pixel is installed, many common browsers will attach third-party cookies allowing Facebook to link the data collected by Meta Pixel to the specific Facebook user.

153. Alternatively, Facebook can link the data to a user's Facebook account through the "Facebook Cookie."[29] The Facebook Cookie is a workaround to recent cookie-blocking applications used to prevent websites from tracking users.[30]

154. Facebook can also link user data to Facebook accounts through information collected through Meta Pixel through what Facebook calls "Advanced Matching." There are two forms of Advanced Matching: manual matching and automatic matching. Manual matching requires the website developer to manually send data to Facebook so that users can be linked to data. Automatic matching allows Meta Pixel to scour the data it receives from third-party websites to search for recognizable fields, including names and email addresses that correspond with users' Facebook accounts.

155. While the Meta Pixel tool "hashes" personal data—obscuring it through a form of cryptography before sending the data to Facebook—that hashing does not prevent *Facebook* from using the data. In fact, Facebook explicitly uses the hashed information it gathers to link pixel data to Facebook profiles.[31]

156. Facebook also receives personally identifiable information in the form of user's unique IP addresses that stay the same as users visit multiple websites. When browsing a third-party website that has embedded Facebook code, a user's unique IP address is forwarded to

[29] https://clearcode.cc/blog/facebook-first-party-cookie-adtech/
[30] https://clearcode.cc/blog/difference-between-first-party-third-party-cookies/
[31] https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites

Facebook by GET requests, which are triggered by Facebook code snippets. The IP address enables Facebook to keep track of the website page visits associated with that address.

157. Facebook also places cookies on visitors' computers. It then uses these cookies to store information about each user. For example, the "c_user" cookie is a unique identifier that identifies a Facebook user's ID. The c_user cookie value is the Facebook equivalent of a user identification number. Each Facebook user has one—and only one—unique c_user cookie. Facebook uses the c_user cookie to record user activities and communications.

158. An unskilled computer user can obtain the c_user value for any Facebook user by (1) going to the user's Facebook page, (2) right-clicking with their mouse anywhere on the background of the page, (3) selecting 'View page source,' (4) executing a control-F function for "user=" and (5) copying the number value that immediately follows "user=" in the page source code of the target Facebook user's page.

159. It is even easier to find the Facebook account associated with a c_user cookie: one simply needs to log-in to Facebook, and then type www.facebook.com/#, with # representing the c_user cookie identifier. For example, the c_user cookie value for Mark Zuckerberg is 4. Logging in to Facebook and typing www.facebook.com/4 in the web browser retrieves Mark Zuckerberg's Facebook page: www.facebook.com/zuck.

160. The datr cookie identifies the patient's specific web browser from which the patient is sending the communication. It is an identifier that is unique to the patient's specific web browser and is therefore a means of identification for Facebook users. Facebook keeps a record of every datr cookie identifier associated with each of its users, and a Facebook user can obtain a redacted list of all datr cookies associated with his or her Facebook account from Facebook.

161. The fr cookie is a Facebook identifier that is an encrypted combination of the c_user and datr cookies.[32]

162. The fbp cookie is a Facebook identifier that is set by Facebook source code and associated with Geisinger's use of the Facebook Tracking Pixel program. The fbp cookie emanates from Geisinger's web properties as a putative first-party cookie, but is transmitted to Facebook through cookie syncing technology that hacks around the same-origin policy.

163. Similarly, the "lu" cookie identifies the last Facebook user who logged in using a specific browser. Like IP addresses, cookies are included with each request that a user's browser makes to Facebook's servers. Facebook employs similar cookies such as the "fr," "act," "presence," "spin," "wd," "xs," and "fbp" cookies to track users on websites across the internet.[33] These cookies allow Facebook to easily link the browsing activity of its users to their real-world identities, and such highly sensitive data as medical information, religion, and political preferences.[34]

164. Facebook also uses browser fingerprinting to uniquely identify individuals. Web browsers have several attributes that vary between users, like the browser software system, plugins that have been installed, fonts that are available on the system, the size of the screen, color depth, and more. Together, these attributes create a fingerprint that is highly distinctive. The likelihood that two browsers have the same fingerprint is at least as low as 1 in 286,777, and the accuracy of the fingerprint increases when combined with cookies and the user's IP address. Facebook recognizes a visitor's browser fingerprint each time a Facebook button is loaded on a third-party

---

[32] *See* Gunes Acar, Brendan Van Alsenoy, Frank Piessens, Claudia Diaz, and Bart Preneel, *Facebook Tracking Through Social Plug-ins: Technical Report prepared for the Belgian Privacy Commission* (March 27, 2015) (available at https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_pluginsv1.0.pdf).

[33] https://techexpertise.medium.com/facebook-cookies-analysis-e1cf6ffbdf8a#:~:text=browser%20session%20ends.-,%E2%80%9Cdatr%E2%80%9D,security%20and%20site%20integrity%20features.

[34] https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf

website page. Using these various methods, Facebook can identify individual users, watch as they browse third-party websites like https://www.geisinger.org/, and target users with advertising based on their web activity.

D. Geisinger has discretely embedded the Meta Pixel tool on its website, resulting in the capture and disclosure of patients' protected health information to Facebook.

165. A third-party website that incorporates Meta Pixel benefits from the ability to analyze a user's experience and activity on the website to assess the website's functionality and traffic. The third-party website also gains information from its customers through Meta Pixel that can be used to target them with advertisements, as well as to measure the results of advertising efforts.

166. Facebook's intrusion into the personal data of visitors to third-party websites incorporating the Meta Pixel is both significant and unprecedented. When Meta Pixel is incorporated into a third-party website, unbeknownst to users and without their consent, Facebook gains the ability to surreptitiously gather every user interaction with the website ranging from what the user clicks on to the personal information entered on a website search bar. Facebook aggregates this data against all websites. Facebook benefits from obtaining this information because it improves its advertising network, including its machine-learning algorithms and its ability to identify and target users with ads.

167. Facebook provides websites using Meta Pixel with the data it captures in the "Meta Pixel page" in Events Manager, as well as tools and analytics to reach these individuals through future Facebook ads. For example, websites can use this data to create "custom audiences" to target the specific Facebook user, as well as other Facebook users who match "custom audience's" criteria. Businesses that use Meta Pixel can also search through Meta Pixel data to find specific types of users to target, such as men over a certain age.

168. Businesses install the Meta Pixel software code to help drive and decode key performance metrics from visitor traffic to their websites.[35] Businesses also use the Meta Pixel to build custom audiences on Facebook that can be used for advertising purposes.[36]

169. For example, when a user on many hospital websites clicks on a "Schedule Online" button next to a doctor's name, Meta Pixel sends the text of the button, the doctor's name, and the search term (such as "cardiology") used to find the doctor to Facebook. If the hospital's website has a drop-down menu to select a medical condition in connection with locating a doctor or making an appointment, that condition is also transmitted to Facebook through Meta Pixel.

170. Facebook has designed the Meta Pixel such that Facebook receives information about patient activities on hospital websites as they occur in real time. Indeed, the moment that a patient takes any action on a webpage that includes the Meta Pixel—such as clicking a button to register, login, logout, or to create an appointment—Facebook code embedded on that page redirects the content of the patient's communications to Facebook while the exchange of information between the patient and hospital is still occurring.

171. Geisinger is among the hospital systems who embedded Meta Pixel on their websites. Via its use of the Meta Pixel, Geisinger intercepted and disclosed the contents of Plaintiff's and Class Members' communications with Geisinger, including the precise text of patient search queries and communications about specific doctors, communications about medical conditions and treatments, and buttons clicked to Search, Find a Doctor, connect, Login, or Enroll in Geisinger's patient portal, summaries of Geisinger's responsive communications, the parties to the communications, and the existence of communications at Geisinger's websites

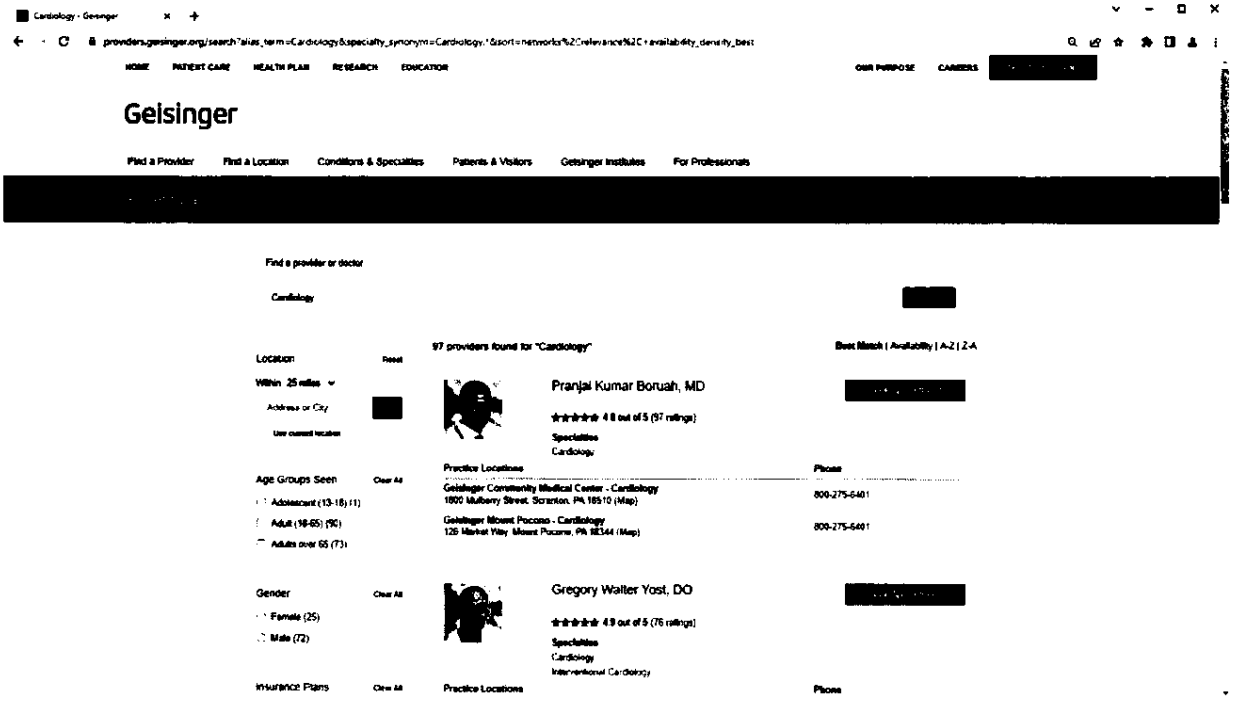
172. For example, when a patient visited the homepage of Geisinger's website, the

[35] https://instapage.com/blog/meta-pixel
[36] https://instapage.com/blog/meta-pixel

source code employed by Geisinger caused personally identifiable information to be transmitted to Facebook and Google.

173. Many of the tabs provided by Geisinger on its website are specific to patients—i.e., "Find a Provider," "Pay Your Bill Online," "Prepare for Your Visit," "Refill a Prescription" and "Sign into MyGeisinger" among others (collectively, "Patient Tabs"). Clicking on any of the Patient Tabs identifies the person using the website as a patient.

174. For example, when a patient entered their personal information through Geisinger's websites that incorporate Meta Pixel, such as to locate a doctor or make an appointment, this information, including what the patient is being treated for, those communications were simultaneously disclosed to Facebook via the Meta Pixel. The acquisition and disclosure of these communications occurred contemporaneously with the transmission of these communications by patients.



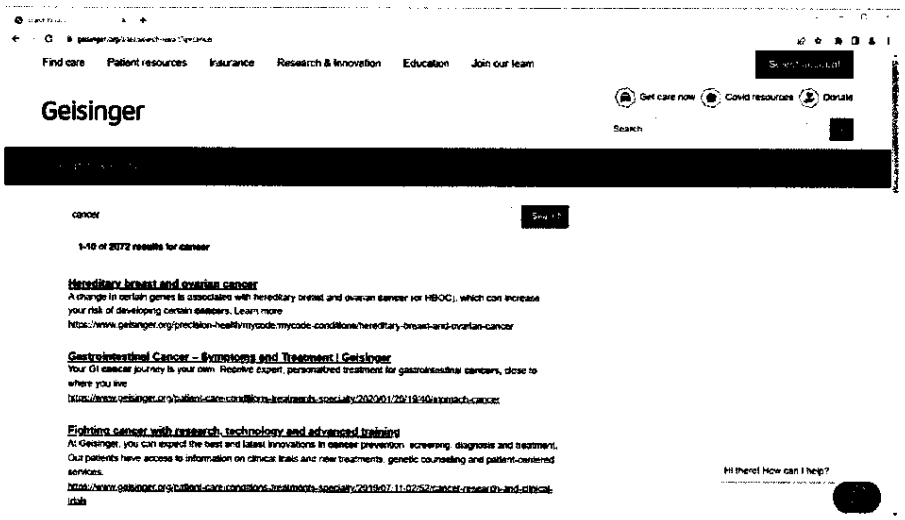
175. This data, which can include health conditions (e.g., addiction, Alzheimer's, heart

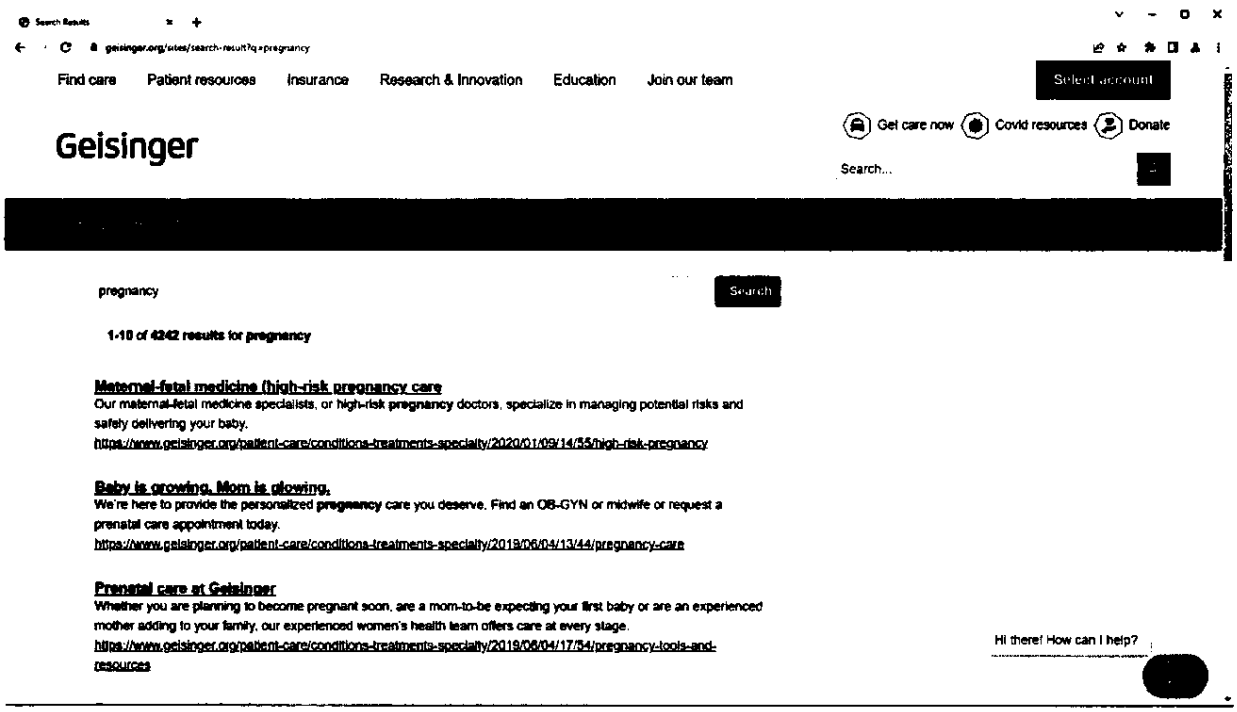
disease), diagnoses, procedures, test results, the treating physician, medications, and other personally identifiable and health information is obtained and used by Facebook, as well as other parties, for the purpose of targeted advertising.

176. All this data was disclosed to Facebook simultaneously in real time as patients transmitted their information, along with other data, such as a patient's unique Facebook ID that is captured by the c_user cookie, which allows Facebook to link this information to patients' unique Facebook accounts. Geisinger also discloses other personally identifiable information to Facebook, such as patient IP addresses, cookie identifiers, browser-fingerprints, URLs, device identifiers, and other unique identifiable characteristics and/or codes.

177. Geisinger caused similar data transmissions to be sent to Facebook and Google with every communication that a patient sends using the Patient Tabs.

178. Geisinger disclosed such personally identifiable information and sensitive medical information even when patients are searching for doctors on its websites to assist with conditions such as cancer or pregnancy.



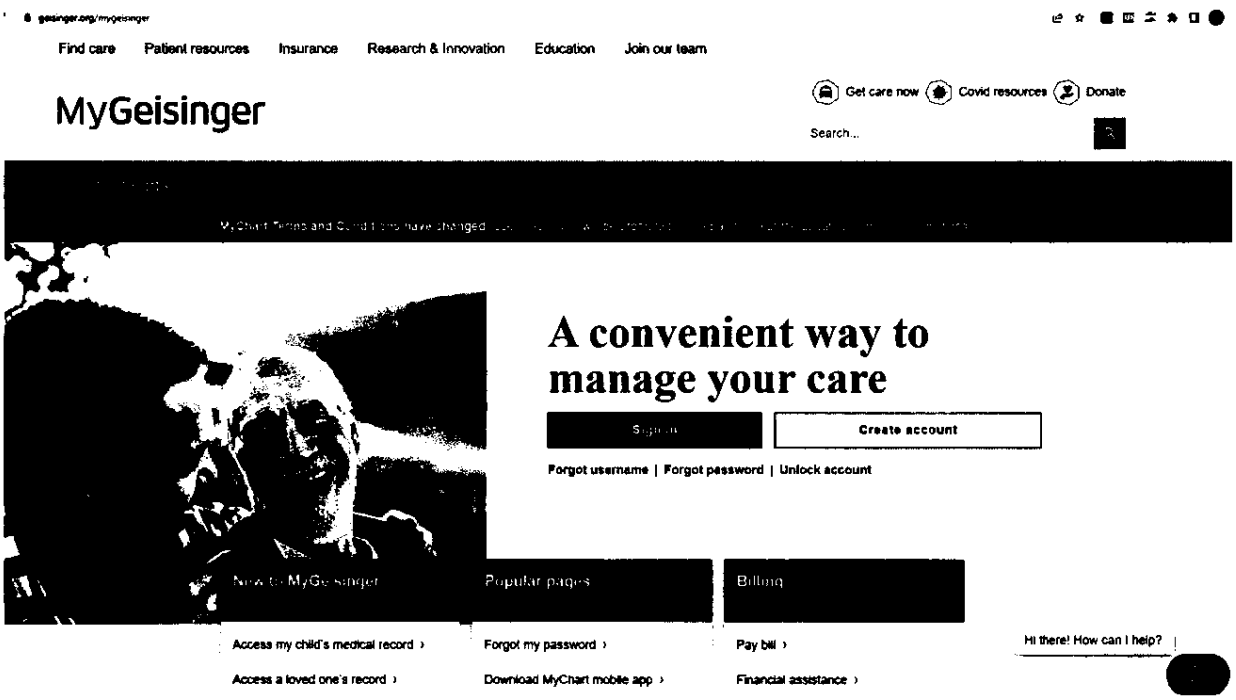


179. When a patient sends a communication searching for more information about "pregnancy" (or any other search), Geisinger caused data transmissions to be made to third parties, including Facebook and Google, that include personal health information, including personally identifiable information and the content of the patient's communications.

180. In other words, Facebook learns not just that patients are seeking treatment, but where and typically when they are seeking treatment, along with other information that patients would reasonably assume that Geisinger is not sharing with third party marketing companies.

181. Geisinger also maintains a patient portal for patients to communicate with Geisinger, with options to do things such as access test results, check appointments, review prescriptions, and communicate with health care providers.

182. Geisinger maintains the login for its patient portal on its website located at https://www.geisinger.org/mygeisinger:



183. Geisinger installed tracking pixels, including Google analytics tracking tools, to personally identify patients like Plaintiff who clicked to log into Geisinger's patient portal.

184. Every Gesinger patient who logs into Geisinger's patient portal from Geisinger's website does so through clicking on the "Sign In" button on Geisinger's website. When patients click the "Sign In" button to access Geisinger's patient portal, Geisinger discloses patients' personal health information, including their status as patients and their personally identifiable information, to multiple third parties including Google.

185. Likewise, Geisinger also maintains a button on its "Patient Resources" tab entitled "Sign Into MyGeisinger," allowing patients to click through to the patient portal section of its website:

186. When a patient clicks the "Sign Into MyGeisinger" button, Geisinger uses the patient's personal identifiers by causing the identifiers to be transmitted to Google attached to the fact that patient has attempted to gain access to Geisinger's patient portal. On information and belief, Gesinger made similar disclosures to Facebook via the Meta Pixel prior to July 7, 2022.

187. The specific identifiers that Geisinger used to help Facebook and Google acquire and record patient communications upon the "Sign Into MyGeisinger" button include the patient's IP address and cookie values, including first party cookies that Geisinger shared with Facebook via cookie syncing.

188. Each time a Geisinger patient, including Plaintiff and Class members, clicked on the "Sign Into MyGeisinger" button, Gesinger caused the patient's personal identifiers, including the patient's IP address, to be transmitted to Facebook and Google attached to the fact that the patient has exchanged a communication with Geisinger regarding the patient portal.

189. In addition, through the source code deployed by Geisinger, the cookies that Geisinger used to help Facebook identify patients include (but are not necessarily limited to) cookies named: c_user, datr, fr, and fbp.

190. For example, the fbp cookie is a Facebook identifier that is set by Facebook source code and associated with Geisinger's use of the Facebook Tracking Pixel program. The fbp cookie emanates from Geisinger's web properties as a putative first-party cookie, but is transmitted to Facebook through cookie syncing technology that hacks around the same-origin policy.

191. On information and belief, the Geisinger patient portal is designed to permit the deployment of custom analytics scripts within the patient portal, including Google Analytics, which allows for the transmission of patients' personal health information, including medical and health-related information, and communications to third parties.

192. On information and belief, Geisinger took advantage of the patient portal's analytics compatibility by knowingly and secretly deploying Google source code inside its patient portal that caused the contemporaneous unauthorized transmission of personally health information and the precise content of patient communications with Geisinger to be sent to Google whenever a patient used the patient portal.

193. Geisinger discloses patient information from across its website including (but not limited to) communications that are captured by the website's search bar, communications that are captured when a patient searches for services offered by Geisinger, communications made by patients using the website's Bill Pay/financials function, communications made when patients access Geisinger's patient portal, and communications made when patients are researching specific medical conditions such as COVID-19.

194. Despite its own legal obligations and internal policies, Geisinger's source code causes the interception and transmission of the following personally identifiable information ("PII") to third parties whenever a patient uses Geisinger's web properties, including Geisinger's patient portal:

a. Patient IP addresses;

b. Unique, persistent patient cookie identifiers;

c. Device identifiers;

d. Account numbers;

e. URLs;

f. Other unique identifying numbers, characteristics, or codes, including patients' Facebook IDs; and

g. Browser-fingerprints.

195. To make the transmissions of patient information and communications to Facebook and Google, Geisinger deployed Facebook and Google source code on its web properties.

196. The Geisinger-deployed source code did the following things:

a. Without any action or authorization, Geisinger deposited cookies such as the _fbp, _ga, and _gid cookies onto Plaintiff's and patient Class members' computing devices. These are cookies associated with the third-parties Facebook and Google but which Geisinger deposits on Plaintiff's and Class members' computing devices by disguising them as first-party cookies.

b. Without any action or authorization, Geisinger's source code commanded Plaintiff's and Class members' computing devices to contemporaneously re-direct the Plaintiff's and Class members' identifiers and the content of their communications to Facebook, Google, and others.

197. Whenever a patient uses Geisinger's web properties, Geisinger intercepts, causes transmission of, and uses personally identifiable patient data without patient knowledge, consent, authorization, or any further action by the patient.

198. Geisinger disclosed Plaintiff's and Class members' personally identifiable patient data, including their status as patients and the contents of their communications with Geisinger, to third parties including Facebook and Google.

199. Geisinger made such unauthorized disclosures to multiple third parties, including Google, Facebook, Kyruus, Salesforce, and New Relic. The disclosures included information that identifies Plaintiff and Class members as Geisinger patients and aids the third parties in receiving and recording patient communications pertaining to or about specific doctors, conditions, treatments, payments, and connections to Geisinger's patient portal.

200. As the above demonstrates, knowing what information a patient is reviewing on Geisinger's website can reveal deeply personal and private information. For example, a simple search for "pregnancy" on Geisinger's website allows Meta Pixel to capture that search term and tell Facebook that the patient is likely pregnant. Indeed, Facebook might learn that the patient is pregnant before the patient's close family and friends. But there is nothing visible on Geisinger's website that would indicate to patients that, when they use Geisinger's search function, their personally identifiable data and the precise content of their communications with Geisinger are being automatically captured and made available to Facebook, who can then use that information for advertising purposes even when patients search for treatment options for sensitive medical conditions such as cancer or substance abuse.

201. The amount of data collected is significant. Via the Meta Pixel, when patients interact with its website, Geisinger discloses a full-string, detailed URL to Facebook, which contains the name of the website, folder and sub-folders on the webserver, and the name of the precise file requested. For example, when a patient types a search term into the search bar on Geisinger's website, the website returns links to information relevant to the search term. When patients then click these links, a communication is created that contains a GET request and a full-string detailed URL.

202. Facebook's Meta Pixel collects and forwards this data to Facebook, including the full referral URL (including the exact subpage of the precise terms being reviewed) and Facebook then correlates the URL with the patient's Facebook user ID, time stamp, browser settings, and even the type of browser used. In short, the URLs, by virtue of including the particular document within a website that a patient views, reveal a significant amount of personal data about a patient. The captured search terms and the resulting URLs divulge a patient's medical issues, personal interests, queries, and interests on third-party websites operating outside of Facebook's platform.

203. The transmitted URLs contain both the "path" and the "query string" arising from patients' interactions with Geisinger's websites. The path identifies where a file can be found on a website. For example, take https://providers.geisinger.org/provider/Seth+Ward+Fisher/758432?. Here, the "path" is provider/ Seth+Ward+Fisher/758432?. Similarly, a patient reviewing information about "Services" that Geisinger offers patients such as "Pediatrics" will generate a URL with the path https://www.geisinger.org/patient-care/conditions-treatments-specialty/pediatrics.

204. Likewise, a query string provides a list of parameters. An example of a URL that provides a query string is https://www.geisinger.org/sites/search-result?q=cancer. The query string parameters in this search indicate that a search was done at the Geisinger website for information about cancer. In other words, the Meta Pixel captures information that connects a particular user to a particular healthcare provider.

205. The contents of patients' search terms shared with Facebook plainly relate to (and disclose) the past, present, or future physical or mental health or condition of individual patients who interact with Geisinger's website. Worse, no matter how sensitive the area of the Geisinger's

website that a patient reviews, the referral URL is acquired by Facebook along with personally identifiable information.

206. The nature of the collected data is also important. Geisinger's unauthorized disclosures result in Facebook obtaining a comprehensive browsing history of an individual patient, no matter how sensitive the patient's medical condition. Facebook is then able to correlate that history with the time of day and other user actions on Geisinger's website. This process results in Facebook acquiring a vast repository of personal data about patients—all without their knowledge or consent.

207. Geisinger also discloses the same kind of patient data described above to other third parties, including Google, Marketo, and LinkedIn via tracking software that Geisinger has installed on its website. As with the Facebook Meta Pixel, Geisinger provides patients and prospective patients with no notice that Geisinger is disclosing the contents of their communications to these third parties. Likewise, Geisinger does not obtain consent from patients and prospective patients before forwarding their communications to these companies.

208. These disclosures to third parties other than Facebook are equally disturbing. Google Analytics, for example, has been described by the Wall Street Journal as "far and away the web's most dominant analytics platform," which "tracks you whether or not you are logged in."[37] Like Facebook, Google tracks internet users with IP addresses, cookies, geolocation, and other unique device identifiers. Geisinger routinely discloses patients' personal health information to such Google services as Google Analytics and Google Tag Manager.

[37] https://www.wsj.com/articles/who-has-more-of-your-personal-data-than-facebook-try-google-1524398401

209. Google cookies are personally identifiable. For example, Google cookies called 'SID' and 'HSID' contain digitally signed and encrypted records of a user's Google account ID and most recent sign-in time.

210. Most people who use Google services have a preferences cookie called 'NID' in their browsers. When you visit a Google service, the browser sends this cookie with your request for a page. The NID cookie contains a unique ID Google uses to remember your preferences and other information.

211. Google uses cookies like NID and SID to help customize ads on Google properties, like Google Search. For example, Google uses such cookies to remember your users' most recent searches, previous interactions with an advertiser's ads or search results, and visits to an advertiser's website. This helps Google show customized ads to users on Google.

212. Google also uses one or more cookies for advertising it serves across the web. One of the main advertising cookies on non-Google sites is named 'IDE' and is stored in browsers under the domain doubleclick.net. Another is stored in google.com and is called ANID. Google also uses other cookies with names such as DSID, FLC, AID, TAID, and exchange_uid. Other Google properties, like YouTube, may also use these cookies to show users ads.

213. Google cookies provide personally identifiable data about patients who visit Geisinger's website to Google. Geisinger transmits personally identifiable Google cookie data to Google.

214. Google warns web-developers that Google marketing tools are not appropriate for health-related webpages and websites. Indeed, Google warns web developers that "Health" is a prohibited category that should not be used by advertisers to target ads to users or promote advertisers' products or services.

215. Google provides instructions for web developers to anonymize IP addresses when they use Google Analytics. Google explains that the IP anonymization feature "is designed to help site owners comply with their own privacy policies or, in some countries, recommendations from local data protection authorities, which may prevent the storage of full IP address information." The Google IP anonymization instructions tell web developers to add a parameter called 'aip' in their Google Analytics source code. When 'aip' ("anonymize IP") is turned on, it will be reported to Google Analytics in a GET request with the following: '&aip=1'.

216. Upon information and belief, Geisinger does not use Google's IP anonymization tool with Google Analytics. As a result, Geisinger's use of Google Analytics is not anonymous, even when no cookies are involved in the re-direction of a patient's communication.

217. Geisinger deploys Google tracking tools on nearly every page of its websites, resulting in the disclosure of communications exchanged with patients to be transmitted to Google. These transmissions occur simultaneously with patients' communications with Geisinger and include communications that Plaintiff and Class Members made about specific medical providers, treatments, conditions, appointments, payments, and registrations and logins to Geisinger's patient portal.

218. By compelling visitors to its websites to disclose personally identifiable data and sensitive medical information to Facebook and other third parties, Geisinger knowingly discloses information that allows Facebook and other advertisers to link its patients' personal health information to their private identities and target them with advertising. Geisinger intentionally shares the personal health information of its patients with Facebook in order to gain access to the benefits of the Meta Pixel tool.

219. Geisinger facilitated the disclosure of Plaintiff's Personal Health information,

including sensitive medical information, to Facebook without her consent or authorization when she entered information on the websites that Geisinger maintains.

220. For example, Plaintiff Jane Doe has a Facebook account and has also been a Geisinger patient for more than 10 years. Plaintiff Jane Doe has regularly used Geisinger's website and patient portal for more than 10 years. Plaintiff Jane Doe regularly entered data on Geisinger's website and patient portal, including sensitive medical information, such as details about her medical condition and doctor. The information that Plaintiff transmitted included queries about treatment for asthma and back pain and potential treating physicians. After entering her medical information on Geisinger's website, Plaintiff began receiving ads on her Facebook page related to her medical condition, including advertisements for pain management and back pain treatments.

221. Plaintiff also regularly used Geisinger's patient portal to do things such as review lab results and diagnoses, review prescription information, and review communications from her doctors.

222. Plaintiff believed that her interactions with Geisinger's website were private and would not be shared with anyone besides her healthcare providers. Plaintiff was dismayed when she learned that Geisinger's website had been capturing her personal health information and disclosing that information to Facebook and Google without consent.

223. The information that Defendant disclosed about Plaintiff to Facebook, permitted Facebook to ascertain her identity, location, and interest in obtaining treatment for asthma and back pain. This information could then be combined with other information in Facebook's possession, like her name, date of birth, and phone number, to more effectively target Plaintiff with advertisements or sell Plaintiff's data to third parties.

224. Because Geisinger embedded the Meta Pixel on its website, Geisinger disclosed

intimate details about Plaintiff's interactions with its website. Each time the Meta Pixel was triggered, it caused Plaintiffs' information to be secretly transmitted to Facebook's servers, as well as additional information that captures and discloses the communications' content and Plaintiff's identity. For example, when Plaintiff and Class Members visited Geisinger's website, their personal health information was transmitted to Facebook, including such engagement as using the website's search bar, using the website's Find A Provider function, and typing content into online forms. During these same transmissions, Geisinger's website would also provide Facebook with Plaintiff's and Class Members' Facebook ID, IP addresses, device IDs, and other information that Plaintiff and Class Members provided. This is precisely the type of information that state and federal law require healthcare providers to de-identify to protect the privacy of patients.

225. Geisinger knew that by embedding Meta Pixel—a Facebook advertising tool—it was permitting Facebook to collect, use, and share Plaintiff's and the Class Members' personal health information, including sensitive medical information and personally identifiable data. Geisinger was also aware that such information would be shared with Facebook simultaneously with patients' interactions with its websites. Geisinger made the decision to barter its patients' personal health information to Facebook because it wanted access to the Meta Pixel tool. While that bargain may have benefited Geisinger and Facebook, it also betrayed the privacy rights of Plaintiff and Class Members.

F. Plaintiff and the Class Members did not consent to the interception and disclosure of their protected health information.

226. Plaintiff and Class Members had no idea when they interacted with Geisinger's websites that their personal data, including sensitive medical data, was being collected and simultaneously transmitted to Facebook. That is because, among other things, Meta Pixel is secretively and seamlessly integrated into Geisinger's websites and is invisible to patients visiting

those websites.

227. For example, when Plaintiff visited Geisinger's website at https://www.geisinger.org/ there was no indication that the Meta Pixel was embedded on that website or that it would collect and transmit her sensitive medical data to Facebook.

228. Plaintiff and her fellow Class Members could not consent to Geisinger's conduct when there was no indication that their sensitive medical information would be collected and transmitted to Facebook in the first place.

229. While Geisinger purports to have privacy policies and notices, the links to those policies and notices are buried at the very bottom of the home page of Geisinger's website so as to be effectively hidden from patients.[38]

230. Even if a patient visiting Geisinger's website located the "Privacy Policy," or the "Notice of Privacy Practices," nothing in any of those pages would have been understood by any reasonable patient to mean that Geisinger's website routinely captured and exploited patients' personal health information, including by sharing that information with Facebook and Google.[39]

231. To the contrary, neither Geisinger's Privacy Policy nor its Notice of Privacy Practices mention the Meta Pixel. [40] Indeed, Geisinger's Privacy Policy expressly states that "Maintaining your trust is important to us. We take your privacy seriously …"[41] Geisinger's Notice of Privacy Practices state that "We will not share your PHI for marketing purposes … without an authorization." [42]

---

[38] https://www.geisinger.org/
[39] https://www.geisinger.org/about-geisinger/corporate/corporate-policies/website-privacy-policy. https://www.geisinger.org/about-geisinger/corporate/corporate-policies/hipaa/notice-of-privacy-practices-ghs.
[40] https://www.geisinger.org/about-geisinger/corporate/corporate-policies/website-privacy-policy. https://www.geisinger.org/about-geisinger/corporate/corporate-policies/hipaa/notice-of-privacy-practices-ghs.
[41] https://www.geisinger.org/about-geisinger/corporate/corporate-policies/website-privacy-policy.
[42] https://www.geisinger.org/about-geisinger/corporate/corporate-policies/hipaa/notice-of-privacy-practices-ghs.

232. These statements are false, deceptive, and misleading in light of Geisinger's secret disclosure of patient information to numerous third parties, including Facebook and Google. Geisinger's privacy policy is also false, deceptive, and misleading because Geisinger in fact routinely sell and/or barter their patients' personal health information to third parties without patients' knowledge or consent in return for access to third party advertising tools.

233. What's more, the very term "Privacy Policy" is deceptive. Research has consistently shown that a majority of Americans who see that a website has a "Privacy Policy" falsely believe that the company with the policy cannot (and will not) disclose information about them to third parties without their consent.

234. Geisinger does not have a legal right to share Plaintiff's and Class Members' Protected Health Information without their written consent to third parties, because this information is protected from such disclosure by law. *E.g.,* 71 P.S. § 1690.108; 45 C.F.R. § 164.508. Nor is Geisinger permitted to disclose patients' Protected Health Information to advertising and marketing companies like Facebook without express written authorization from patients. 28 Pa. Code § 115.27; 31 Pa. Code § 146b.12(a).

235. Indeed, the United States Department of Health and Human Services ("HHS") recently confirmed that hospitals are prohibited from transmitting individually identifiable health information via tracking technology like the Meta Pixel without a patient's authorization and other protections like a business associate agreement with the recipient of the patient data.[43] Among other things, the HHS warned hospitals like Defendant that "Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. For example, disclosures

[43] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html

of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures."[44]

236. Geisinger failed to obtain a valid written authorization from Plaintiff or any of the Class Members to allow the capture and exploitation of their personally identifiable information and the contents of their communications for marketing purposes.

237. A patient's reasonable expectation that their health care provider will not share their information with third parties for marketing purposes is not subject to waiver via an inconspicuous privacy policy hidden away on a company's website. Further, Geisinger expressly promised its patients that it would never sell or use their personal health information without express authorization.

238. Accordingly, Geisinger lacked authorization to intercept, disclose to Facebook, or use Plaintiff and Class Members' personal health information, or to procure others (such as Facebook) to intercept, disclose, or use such personal health information.

G. Geisinger's disclosures of personal patient data to Facebook are unnecessary.

239. There is no information anywhere on the websites operated by Geisinger that would alert patients that their most private information (such as their identifiers, their medical conditions, and their medical providers) is being automatically transmitted to Facebook. Nor are any of the disclosures of patient personal health information to Facebook necessary for Geisinger to maintain its healthcare website or provide medical services to patients.

240. For example, it is possible for a healthcare website to provide a doctor search function without allowing disclosures to third-party advertising companies about patient sign ups or appointments. It is also possible for a website developer to utilize tracking tools without

[44] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html

allowing disclosure of patients' Personal Healthcare Information to companies like Facebook. Likewise, it is possible for Geisinger to provide medical services to patients without sharing their personal health information with Facebook so that this information can be exploited for advertising purposes.

241. Despite these possibilities, Geisinger willfully chose to implement Meta Pixel on its websites and aid in the disclosure of personally identifiable information and sensitive medical information about its patients, as well as the contents of their communications with Geisinger, to third-parties, including Facebook.

H. Plaintiff and Class Members have a reasonable expectation of privacy in their personal health information, especially with respect to sensitive medical information.

242. Patient personal health information is specifically protected by law. *E.g.* 28 Pa. Code § 115.27; 28 Pa. Code § 563.9; 28 Pa. Code § 710.23. The prohibitions against disclosing patient personal health information include prohibitions against disclosing personally identifiable information such as patient names, IP addresses, and other unique characteristics or codes. *E.g.* 49 Pa. Code § 16.61(a)(1); 45 C.F.R. § 164.514. Both state and federal law also restrict the use of patients' Personal Health information, including their status as patients, to only those uses related to their care unless patients have provided express written authorization to the contrary.

243. Plaintiff and Class Members have a reasonable expectation of privacy in their personal health information, including personally identifiable data and sensitive medical information. Geisinger's surreptitious interception, collection, and disclosure of patients' personal health information to Facebook violated Plaintiff and Class Member's privacy interests.

244. As patients, Plaintiff and Class Members had a reasonable expectation of privacy that their health care provider and its associates would not disclose their personal health information to third parties without their express authorization. Those expectations are derived

from multiple sources, including (a) Geisinger's status as Plaintiff and Class Members health care provider, (b) Geisinger's common law obligations to maintain the confidentiality of patient data and communications, (c) state and federal laws and regulations protecting the confidentiality of medical information, (d) state and federal laws protecting the confidentiality of electronic communications and computer data, (e) state laws protecting unauthorized use of personal means of identification, (f) Geisinger's express promises of confidentiality, and (g) Geisinger's implied promises of confidentiality.

245. The original Hippocratic Oath, circa 400 B.C., provided that physicians must pledge, "What I may see or hear in the course of treatment or even outside of the treatment in regard to the life of man, which on no account must be spread abroad, I will keep to myself holding such things shameful to be spoken about."[45]

246. The modern Hippocratic Oath provides, "I will respect the privacy of my patients, for their problems are not disclosed to me that the world may know."[46] Likewise, the American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications. For example, the AMA has issued medical ethics opinions providing that "[p]rotecting information gathered in association with the care of a patient is a core value in health care. However, respecting patient privacy in other forms is also fundamental, as an expression of respect for patient autonomy and a prerequisite for trust....Physicians must seek to protect patient privacy in all settings to the greatest extent possible and should ... [m]inimize intrusion on privacy when the patient's privacy must be balanced against other factors [and inform] the patient when there has been a significant infringement on privacy of

[45] *Brandt v. Medical Defense Associates*, 856 S.W.2d 667, 671 n.1 (Mo. 1993).
[46] https://www.pbs.org/wgbh/nova/doctors/oath_modern.html

which the patient would otherwise not be aware."[47]

247. The AMA's ethics opinions have further cautioned physicians and hospitals that "[d]isclosing information to third parties for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship." [48]

248. Plaintiff's and Class Members' reasonable expectations of privacy in their personal health information are grounded in, among other things, Geisinger's status as a health care provider, Geisinger's common law obligation to maintain the confidentiality of patients' personal health information, state and federal laws protecting the confidentiality of medical information, state and federal laws protecting the confidentiality of communications and computer data, state laws prohibiting the unauthorized use and disclosure of personal means of identification, and Geisinger's express and implied promises of confidentiality.

249. It was reasonable for Plaintiff and Class Members to assume that Geisinger's privacy policies were consistent with Geisinger's duties to protect the confidentiality of patients' personal health information.

250. Indeed, multiple studies examining the collection and disclosure of consumers' sensitive medical information confirm that the disclosure of sensitive medical information violates expectations of privacy that have been established as general social norms.

251. Privacy polls and studies also uniformly show that the overwhelming majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its customers' data.

---

[47] https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/code-of-medical-ethics-chapter-3.pdf (opinion 3.1.1).

[48] https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/code-of-medical-ethics-chapter-3.pdf (opinion 3.2.4).

252. For example, a recent study by *Consumer Reports* showed that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumers' data, and the same percentage believed that internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.[49]

253. Users act consistently with these preferences. For example, following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85 percent of worldwide users and 94 percent of U.S. users chose not to share data when prompted.[50]

254. "Patients are highly sensitive to disclosure of their health information," particularly because it "often involves intimate and personal facts, with a heavy emotional overlay." Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, 33 RUTGERS L.J. 617, 621 (2002). Unsurprisingly, empirical evidence demonstrates that "[w]hen asked, the overwhelming majority of Americans express concern about the privacy of their medical records." Sharona Hoffman & Andy Podgurski, *E-Health Hazards: Provider Liability and Electronic Health Record Systems*, 24 BERKELEY TECH L.J. 1523, 1557 (2009).

255. The concern about sharing personal medical information is compounded by the reality that advertisers view this type of information as particularly valuable. Indeed, having access to the data women share with their healthcare providers allows advertisers to obtain data on children before they are even born. As one recent article noted, "What is particularly worrying about this process of datafication of children is that companies like [Facebook] are harnessing and

[49] https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/
[50] https://www.wired.co.uk/article/apple-ios14-facebook

collecting multiple typologies of children's data and have the potential to store a plurality of data traces under unique ID profiles."[51]

256. Many privacy law experts have expressed serious concerns about patients' sensitive medical information being disclosed to third-party companies like Facebook. As those critics have pointed out, having a patient's personal health information disseminated in ways the patient is unaware of could have serious repercussions, including affecting their ability to obtain life insurance, how much they might pay for such coverage, the rates they might be charged on loans, and the likelihood of their being discriminated against.

I. Plaintiff and Class Members did not receive the benefit of the bargain they had with Geisinger.

257. Geisinger does not generally provide its medical services for free. All Geisinger patients, including Plaintiff, pay Geisinger either directly or indirectly (e.g. through insurance, which they pay for) for medical services. The fees Geisinger charges may be itemized to a certain degree, for example the charges may be separated by treatment or medical procedure. But even at their most itemized level, those charges cover a wide range of services that Geisinger is providing with respect to any given treatment.

258. For example, patients do not receive a separate charge for the dressing gown they wear before surgery. Yet clearly that dressing gown has real value and is part of medical services that Geisinger provides to a surgery patient, and therefore the fee charged for the surgery reflects the value of that dressing gown, even though it is not separately itemized on their bill. If Geisinger told its patients that such items would be covered as part of their surgery, and yet Geisinger then made the patient separately purchase a gown in the hospital lobby before surgery, that patient clearly would not have received the benefit of the bargain struck with Geisinger.

[51] https://thereader.mitpress.mit.edu/tech-companies-are-profiling-us-from-before-birth/

259. So too, when Geisinger purports to provide its patients with a modern, convenient and secure means of obtaining medical services, including scheduling appointments, communicating with doctors, and obtaining test results, that is an integral part of the medical services that Geisinger provides, that has real value even if it is not separately itemized on a patient's bill.

260. Geisinger touts the convenience and privacy of such services through its patient portal and other web properties. Therefore, when Geisinger failed to follow through in providing the promised level of privacy and security, Geisinger patients (including Plaintiff) did not receive the full benefit of the bargain that they struck with Geisinger when they paid for their medical services.

J. Plaintiff's Personal Health Data that Geisinger collected, disclosed, and used is Plaintiff's property, has economic value, and its illicit disclosure has caused Plaintiff harm.

261. Property is the right of any person to possess, use, enjoy, or dispose of a thing, including intangible things like data and communications. Plaintiff and Class Members have a vested property right in their personal health information.

262. The United States Supreme Court has explained that, "Confidential business information has long been recognized as property." *Carpenter v. United States*, 484 U.S. 19, 26 (1987). "Depriv[ation] of [the] right to exclusive use of … information" causes a loss of property "for exclusivity is an important aspect of confidential business information and most private property for that matter." *Id.* at 27. There is no doubt that Geisinger has a "property right" in patient data such that, if Facebook or Google took such information from Geisinger without authorization, Geisinger would have a claim for Facebook and Google's taking of their property. Patients also have a property right in their own health information that may not be taken or used by Geisinger without their authorization for non-health care related reasons.

263. Federal and state law grant patients the right to protect the confidentiality of data that identifies them as patients of a particular health care provider and restrict the use of their health data, including their status as a patient, to only uses related to their care or otherwise authorized by federal or state law in the absence of patient authorization.

264. A patient's right to protect the confidentiality of their health data and restrict access to it is a valuable right.

265. In addition to property rights in their health data, patients enjoy property rights in the privacy of their health communications.

266. Patient property rights in their health data and communications are established by HIPAA and state health privacy laws that are equally or more stringent than HIPAA.

267. Geisinger's unauthorized acquisition, use, and disclosure of Plaintiff's and Class Members' individually personal health information for marketing purposes violated their property rights to control how their health data and communications are used and who may be the beneficiaries of their data and communications.

268. It is common knowledge that there is an economic market for consumers' personal data—including the kind of data that Geisinger has collected and disclosed from Plaintiff and Class Members. Indeed, the value of data that companies like Facebook and Google extract from people who use the Internet is well understood and generally accepted in the e-commerce industry.

269. Personal information is now viewed as a form of currency. Professor Paul M. Schwartz noted in the Harvard Law Review:

> Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer

> information. Paul M. Schwartz, Property, Privacy and Personal Data, 117 HARV. L. REV. 2055, 2056-57 (2004).

270. For example, in 2013, the *Financial Times* reported that the data-broker industry profits from the trade of thousands of details about individuals, and that within that context, "age, gender and location information" were being sold for approximately "$0.50 per 1,000 people."

271. In a 2021 Washington Post article, the legal scholar Dina Srinivasan said that consumers "should think of Facebook's cost as [their] data and scrutinize the power it has to set its own price." This price is only increasing. According to Facebook's own financial statements, the value of the average American's data in advertising sales rose from $19 to $164 per year between 2013 and 2020.

272. Medical information derived from medical providers garners even more value from the fact that it is not available to third party data marketing companies because of strict restrictions on provider disclosures under HIPAA, state laws, and provider standards, including the Hippocratic oath.

273. The cash value of Internet users' personal health information can be quantified. In a 2015 study by the Ponemon Institute, researchers determined the value that American Internet users place on their "health condition" as more valuable than any other piece of data about them, with a minimum value of $82.90.[52]

274. In 2015, *TechCrunch* reported that "to obtain a list containing the names of individuals suffering from a particular disease," a market participant would have to spend about "$0.30" per name.[53] That same article noted that "Data has become a strategic asset that allows

[52] Ponemon Institute, Privacy and Security in a Connected Life: A Study of US Consumers, March 2015, available at https://vdocuments.site/privacy-and-security-in-a-connected-life-protect-personal-information-from-being.html?page=1.
[53] https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/

companies to acquire or maintain a competitive edge" and that the value of a single user's data can vary from $15 to more than $40 per user.[54]

275. Despite the protections afforded by law, there is an active market for health information. Medical information obtained from health providers garners substantial value because of the fact that it is not generally available to third party data marketing companies because of the strict restrictions on disclosure of such information by state laws and provider standards, including the Hippocratic oath. Even with these restrictions, however, a multi-billion-dollar market exists for the sale and purchase of such private medical information.[55]

276. Further, individuals can sell or monetize their own data if they so choose. For example, Facebook has offered to pay individuals for their voice recordings,[56] and has paid teenagers and adults up to $20 a month plus referral fees to install an app that allows Facebook to collect data on how individuals use their smart phones.[57]

277. A myriad of other companies and apps such as DataCoup, Nielsen Computer, Killi, and UpVoice also offer consumers money in exchange for access to their personal data.[58]

278. Upon information and belief, Geisinger was compensated for its disclosures of Plaintiff's and Class members' personally identifiable patient data and communications by the third-party recipients in the form of enhanced marketing services or other compensation.

---

[54] https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/
[55] https://revealnews.org/blog/your-medical-data-is-for-sale-and-theres-nothing-you-can-do-about-it/; *see also https://slate.com/technology/2022/06/health-data-brokers-privacy.html*
[56] https://www.theverge.com/2020/2/20/21145584/facebook-pay-record-voice-speech-recognition-viewpoints-prounnciations-app
[57] https://www.cnbc.com/2019/01/29/facebook-paying-users-to-install-app-to-collect-data-techcrunch.html
[58] https://www.creditdonkey.com/best-apps-data-collection.html; *see also https://www.monetha.io/blog/rewards/earn-money-from-your-data/*

279. Geisinger did not pay or offer to pay Plaintiff or Class members for their communications or personally-identifiable patient data associated with these disclosures before or after the disclosures were made.

280. Geisinger profited from Plaintiff's and Class members' information without ever intending to compensate Plaintiff and Class members or inform them that the disclosures had been made.

281. Geisinger was unjustly enriched by its conduct.

282. Given the monetary value that data companies like Facebook have already paid for personal information in the past, Geisinger has deprived Plaintiff and the Class Members of the economic value of their sensitive medical information by collecting, using, and disclosing that information to Facebook and other third parties without consideration for Plaintiff and the Class Member's property.

K. Geisinger is enriched by making unlawful, unauthorized, and unnecessary disclosures of its patients' protected health information.

283. In exchange for disclosing personal health information about its patients, Geisinger is compensated by Facebook with enhanced online advertising services, including (but not limited to) retargeting and enhanced analytics functions.

284. Retargeting is a form of online targeted advertising that targets users with ads based on their previous internet actions, which is facilitated through the use of cookies and tracking pixels. Once an individual's data is disclosed and shared with a third-party marketing company, the advertiser is able to show ads to the user elsewhere on the internet.

285. For example, retargeting could allow a web-developer to show advertisements on other websites to customers or potential customers based on the specific communications exchanged by a patient or their activities on a website. Using the Meta Pixel, a website could

target ads on Facebook itself or on the Facebook advertising network. The same or similar advertising can be accomplished via disclosures to other third-party advertisers and marketers.

286. Once personally identifiable information relating to patient communications is disclosed to third parties like Facebook, Geisinger loses the ability to control how that information is subsequently disseminated and exploited.

287. The monetization of the data being disclosed by Geisinger, both by Geisinger and Facebook, demonstrates the inherent value of the information being collected.

L. Facebook's history of egregious privacy violations.

288. Geisinger knew or should have known that Facebook could not be trusted with its patients' sensitive medical information.

289. Due to its ability to target individuals based on granular data, Facebook's ad-targeting capabilities have frequently come under scrutiny. For example, in June 2022, Facebook entered into a settlement with the Department of Justice regarding its Lookalike Ad service, which permitted targeted advertising by landlords based on race and other demographics in a discriminatory manner. That settlement, however, reflected only the latest in a long history of egregious privacy violations by Facebook.

290. In 2007, when Facebook launched "Facebook Beacon," users were unaware that their online activity was tracked, and that the privacy settings originally did not allow users to opt-out. As a result of widespread criticism, Facebook Beacon was eventually shut down.

291. In 2011, Facebook settled charges with the Federal Trade Commission relating to its sharing of Facebook user information with advertisers, as well as its false claim that third-party apps were able to access only the data they needed to operate when—in fact—the apps could access nearly all of a Facebook user's personal data. The resulting Consent Order prohibited

Facebook from misrepresenting the extent to which consumers can control the privacy of their information, the steps that consumers must take to implement such controls, and the extent to which Facebook makes user information available to third parties.[59]

292. Facebook found itself in another privacy scandal in 2015 when it was revealed that Facebook could not keep track of how many developers were using previously downloaded Facebook user data. That same year, it was also revealed that Facebook had violated users' privacy rights by harvesting and storing Illinois' users' facial data from photos without asking for their consent or providing notice. Facebook ultimately settled claims related to this unlawful act for $650 million.[60]

293. In 2018, Facebook was again in the spotlight for failing to protect users' privacy. Facebook representatives testified before Congress that a company called Cambridge Analytica may have harvested the data of up to 87 million users in connection with the 2016 election. This led to another FTC investigation in 2019 into Facebook's data collection and privacy practices, resulting in a record-breaking five-billion-dollar settlement.

294. Likewise, a different 2018 report revealed that Facebook had violated users' privacy by granting access to user information to over 150 companies.[61] Some companies were even able to read users' private messages.

295. In June 2020, after promising users that app developers would not have access to data if users were not active in the prior 90 days, Facebook revealed that it still enabled third-party developers to access this data.[62] This failure to protect users' data enabled thousands of developers to see data on inactive users' accounts if those users were Facebook friends with someone who

[59] https://www.ftc.gov/legal-library/browse/cases-proceedings/092-3184-182-3109-c-4365-facebook-inc-matter
[60] A similar case is pending in Texas.
[61] https://www.cnbc.com/2018/12/19/facebook-gave-amazon-microsoft-netflix-special-access-to-data-nyt.html
[62] https://fortune.com/2020/07/01/facebook-user-data-apps-blunder/

was an active user.

296. On February 18, 2021, the New York State Department of Financial Services released a report detailing the significant privacy concerns associated with Facebook's data collection practices, including the collection of health data. The report noted that while Facebook maintained a policy that instructed developers not to transmit sensitive medical information, Facebook received, stored, and analyzed this information anyway. The report concluded that "[t]he information provided by Facebook has made it clear that Facebook's internal controls on this issue have been very limited and were not effective … at preventing the receipt of sensitive data."[63]

297. The New York State Department of Financial Service's concern about Facebook's cavalier treatment of private medical data is not misplaced. In June 2022, the FTC finalized a different settlement involving Facebook's monetizing of sensitive medical data. In that case, the more than 100 million users of Flo, a period and ovulation tracking app, learned something startling: the company was sharing their data with Facebook.[64] When a user was having her period or informed the app of her intention to get pregnant, Flo would tell Facebook, which could then use the data for all kinds of activities including targeted advertising. In 2021, Flo settled with the Federal Trade Commission for lying to its users about secretly sharing their data with Facebook, as well as with a host of other internet advertisers, including Google, Fabric, AppsFlyer, and Flurry. The FTC reported that Flo "took no action to limit what these companies could do with users' information."[65]

298. More recently, Facebook employees admitted to lax protections for sensitive user

[63] https://www.dfs.ny.gov/system/files/documents/2021/02/facebook_report_20210218.pdf
[64] https://slate.com/technology/2022/06/health-data-brokers-privacy.html
[65] https://slate.com/technology/2022/06/health-data-brokers-privacy.html

data. Facebook engineers on the ad business product team conceded in a 2021 privacy review that "We do not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose."[66]

299. These revelations were confirmed by an article published by the Markup on June 16, 2022, which found during the course of its investigation that Facebook's purported "filtering" failed to discard even the most obvious forms of sexual health information. Worse, the article found that the data that the Meta Pixel was sending Facebook from hospital websites not only included details such as patients' medications, descriptions of their allergic reactions, details about their upcoming doctor's appointments, but also included patients' names, addresses, email addresses, and phone numbers.[67]

300. Despite knowing that the Meta Pixel code embedded in its websites was sending patients' personal health information to Facebook, Geisinger did nothing to protect its patients from egregious intrusions into its patients' privacy, choosing instead to benefit at those patients' expense.

TOLLING, CONCEALMENT, AND ESTOPPEL

301. The applicable statutes of limitation have been tolled as a result of Geisinger's knowing and active concealment and denial of the facts alleged herein.

302. Geisinger seamlessly incorporated Meta Pixel and other trackers into its websites, providing no indication to users that they were interacting with a website enabled by Meta Pixel. Geisinger had knowledge that its websites incorporated Meta Pixel and other trackers yet failed to

[66] https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes
[67] https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites

disclose that by interacting with Meta-Pixel enabled websites that Plaintiff and Class Members' sensitive medical information would be intercepted, collected, used by, and disclosed to Facebook.

303. Meta Pixel is purposefully designed and integrated in a way that makes it impossible to identify with the naked eye and its presence can only be discovered through means significantly more sophisticated than possessed by the average internet user.

304. Plaintiff and Class Members could not with due diligence have discovered the full scope of Geisinger's conduct, because there were no disclosures or other indication that they were interacting with websites employing Meta Pixel and other tracking pixels.

305. Further, Plaintiff and Class Members were not on notice to look for the Meta Pixel, and Geisinger's overt representations assured them that their personal information was being treated in a confidential manner.

306. All applicable statutes of limitation have also been tolled by operation of the discovery rule and the doctrines of fraudulent concealment and continuing tort. Geisinger's illegal interception and disclosure of patients' personal health information has continued unabated through the date of the filing of Plaintiff's Original Complaint. What's more, Geisinger was under a duty to disclose the nature and significance of their data collection practices but did not do so. Geisinger is therefore estopped from relying on any statute of limitations defenses.

CLASS ACTION ALLEGATIONS

307. Plaintiff re-alleges and incorporate by reference the allegations set forth above.

308. Geisinger's conduct violates the law, its duty of confidentiality, its express and implied promises, and Plaintiff's and Class Members' right to privacy.

309. Geisinger's unlawful conduct has injured Plaintiff and Class Members.

310. Geisinger's conduct is ongoing.

311. Plaintiff brings this action individually and as a class action against Geisinger.

312. Plaintiff seeks class certification for the following proposed Class:

> **The Geisinger Class:** During the fullest period allowed by law, all current Pennsylvania citizens who are, or were, patients of Geisinger, or any of its affiliates and who exchanged communications at Geisinger's websites, including https://www.geisinger.org/, and any other Geisinger affiliated website, including Geisinger's patient portal.

313. Excluded from the proposed Class are: (1) any Judge or Magistrate presiding over this action and members of their families; (2) Geisinger, Geisinger's subsidiaries, affiliates, parents, successors, predecessors, and any entity in which the Geisinger or their parents have a controlling interest and their current or former employees, officers, and directors; and (3) Plaintiff's counsel and Geisinger's counsel.

314. Plaintiff reserves the right to redefine the Class and/or add Subclasses at, or prior to, the class certification stage, in response to discovery or pursuant to instruction by the Court.

315. Plaintiff seeks certification of this matter as a class action pursuant to Pennsylvania Rules of Civil Procedure § 1701 *et seq.*

316. **Numerosity:** While the exact number of Class Members is unknown to Plaintiff at this time, the Class, based on information and belief, consists of thousands of people dispersed throughout the Commonwealth of Pennsylvania, such that joinder of all members is impracticable. The exact number of Class Members can be determined by review of information maintained by Geisinger.

317. **Commonality and Predominance:** There are questions of law and fact common to Class Members and which predominate over any questions affecting only individual members. A class action will generate common answers to the questions below, which are apt to drive resolution:

a. Whether Geisinger's acts and practices violated Plaintiff and Class Members' privacy rights;

b. Whether Geisinger's acts and practices violate 18 Pa. C.S. § 5703(1)-(3);

c. Whether Geisinger's acts and practices violate 28 Pa. Code § 115.27;

d. Whether Geisinger's acts and practices violate 49 Pa. Code § 16.61(a)(1);

e. Whether Geisinger's acts and practices violate the duty of doctor-patient confidentiality recognized in *Haddad v. Gopal*, 787 A.2d 975, 980 (Pa. Super. 2001);

f. Whether Geisinger's acts and practices violate 55 Pa. Code § 5100.37;

g. Whether Geisinger's acts and practices violate 28 Pa. Code § 710.23;

h. Whether Geisinger's acts and practices violate 71 P.S. §§ 1690.108(b)(1) & (b)(2);

i. Whether Geisinger's acts and practices violate 50 P.S. § 7111;

j. Whether Geisinger knowingly allowed the surreptitious collection and disclosure of Plaintiff and Class Members' personal health information to Facebook and other third parties;

k. Whether Geisinger's acts and practices constitute a breach of fiduciary duty;

l. Whether Geisinger's acts and practices were intentional;

m. Whether Geisinger profited from disclosures of Plaintiff's and Class Members' personal health information to third parties;

n. Whether Geisinger profited from disclosures of patient personal health information to third parties including Facebook;

o. Whether Geisinger was unjustly enriched;

p. Whether Geisinger's acts and practices harmed and continue to harm Plaintiff and Class Members and, if so, the extent of that injury;

q. Whether Plaintiff and Class Members are entitled to equitable relief including, but not limited to, injunctive relief, restitution, and disgorgement; and

r. Whether Plaintiff and Class Members are entitled to actual, statutory, punitive or other forms of damages, and other monetary relief.

318. These common questions of law and fact predominate over any questions affecting only the individual Class Members.

319. Geisinger engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff individually and on behalf of the other Class Members. Identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

320. **Typicality:** Plaintiff's claims are typical of the claims of other Class Members and Plaintiff have substantially the same interest in this matter as other Class Members. Plaintiff has no interests that are antagonist to, or in conflict with, the interests of other members of the Class. Plaintiff's claims arise out of the same set of facts and conduct as all other Class Members. Plaintiff and all Class Members are patients of Geisinger who used the websites set up by Geisinger for patients and are victims of Geisinger's respective unauthorized disclosures to third parties including Facebook. All claims of Plaintiff and Class Members are based on Geisinger's wrongful conduct and unauthorized disclosures.

321. **Adequacy of Representation:** Plaintiff is committed to prosecuting this action and has retained competent counsel experienced in litigation of this nature. Plaintiff's claims are coincident with, and not antagonistic to, those of other Class Members she seeks to represent. Plaintiff has no disabling conflicts with Class Members. Accordingly, Plaintiff is an adequate representative of the Class and, along with counsel, will fairly and adequately protect the interests of the Class and any Subclasses.

322. **Superiority:** A class action is the superior method for fair and efficient adjudication of the controversy. Although all Class Members have claims against Geisinger, the likelihood that individual Class Members will prosecute separate actions is remote due to the time and expense necessary to conduct such litigation. The damages, harm, and other financial

detriment suffered individually by Plaintiff and other Class Members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Geisinger, making it impractical for Class Members to individually seek redress for Geisinger's wrongful conduct. Moreover, serial adjudication in numerous venues is not efficient, timely, or proper. Judicial resources would be unnecessarily depleted by prosecution of individual claims. The prosecution of separate actions by individual Class Members could create a risk of inconsistent or varying adjudications with respect to individual members of the Cass, which could establish incompatible standards of conduct for Geisinger or adjudications with respect to individual members of the Class which would, as a practical matter, be dispositive of the interests of the members of the Class Members who are not parties to the adjudications. If a class action is not permitted, Class Members will continue to suffer losses and Geisinger's misconduct will continue without proper remedy.

323. Plaintiff anticipates no unusual difficulties in the management of this litigation as a class action. The Class is readily ascertainable and direct notice can be provided from the records maintained by Geisinger, electronically or by publication, the cost of which is properly imposed on Geisinger.

324. For the above reasons, among others, a class action is superior to other available methods for the fair and efficient adjudication of this action.

CAUSES OF ACTION

COUNT I
Violation of Wiretapping and Electronic Surveillance Control Act (WESCA), 18 Pa. C.S. § 5701 *et seq*
(On Behalf of Plaintiff and the Class)

325. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

326. Plaintiff brings this claim on behalf of herself and all members of the Class.

327. All conditions precedent to this action have been performed or have occurred.

328. WESCA prohibits any person from:

a. intentionally intercepting, endeavoring to intercept, or procuring any other person to intercept or endeavor to intercept any wire, electronic or oral communication;

b. intentionally disclosing or endeavoring to disclose to any other person the contents of any wire, electronic or oral communication, if that person knows or has reason to know that the information was obtained through the interception of a wire, electronic or oral communication; or

c. intentionally using or endeavoring to use the contents of any wire, electronic or oral communication, if that person knows or has reason to know that the information was obtained through the interception of a wire, electronic or oral communication.

329. Any person whose wire, electronic, or oral communication is intercepted, disclosed, or used in violation of WESCA "shall have a civil cause of action against any person who intercepts, discloses or uses or procures any other person to intercept, disclose or use, such communication." 18 Pa. C.S. § 5725.

330. Geisinger qualifies as a person under the WESCA. *See* 18 Pa. C.S. §5702.

331. Geisinger has engaged in, and continues to engage in, intentionally intercepting, endeavoring to intercept, or procuring other person(s), including at least Facebook and Google, to intercept or endeavor to intercept, the contents of alleged wire or electronic communications between Plaintiff or Class Members and Geisinger.

332. In addition, or in the alternative, Geisinger has engaged in, and continues to engage in, intentionally disclosing or endeavoring to disclose to other person(s), including at least Facebook, the contents of wire or electronic communications between Plaintiff or Class Members and Geisinger, even though Geisinger person knows, or at least has reason to know,

that the information was obtained through the interception of wire or electronic communications between Plaintiff or Class Members and Geisinger.

333. In addition, or in the alternative, Geisinger has engaged in, and continues to engage in, intentionally using or endeavoring to use the contents of wire or electronic communications between Plaintiff or Class Members and Geisinger, even though Geisinger person knows, or at least has reason to know, that the information was obtained through the interception of wire or electronic communications between Plaintiff or Class Members and Geisinger.

334. All parties to the communications between Plaintiff or Class Members and Geisinger alleged herein have not given prior consent to such interception because Plaintiff or Class Members, as parties to said communications, never gave such consent. *See* 18 Pa. C.S. §5704(4).

335. Plaintiff and Class Members reasonably expected that their personal health information was not being intercepted, recorded, and disclosed to Facebook, Google, and other third parties.

336. No legitimate commercial purpose was served by Geisinger's willful and intentional disclosure of Plaintiff's and Class Members' personal health information to Facebook, Google, and other third parties. Neither Plaintiff nor Class Members consented to the disclosure of their personal health information by Geisinger to Facebook and other third parties. Nor could they have consented, given that Geisinger never sought Plaintiff's or Class Members' consent, much less told visitors to its website that their every interaction was being recorded and transmitted to third parties via tracking tools.

337. Under the WESCA, aggrieved persons such as Plaintiff or Class Members are entitled to recover from Geisinger:

a. actual damages but not less than liquidated damages computed at the rate of $100 per day for each violation or $1,000, whichever is higher;

b. punitive damages; and

c. a reasonable attorney's fee and other litigation disbursements reasonably incurred.

338. In addition to statutory damages, Geisinger's breach caused Plaintiff and Class Members the following damages:

a. Sensitive and confidential information that Plaintiff and Class Members intended to remain private is no longer private;

b. Geisinger eroded the essential confidential nature of the doctor-patient relationship;

c. Geisinger took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without sharing the benefit of such value;

339. Plaintiff and Class Members have also suffered irreparable injury from Geisinger's unauthorized acts of disclosure. Their personal, private, and sensitive data has been collected, viewed, accessed, stored, and used by Geisinger and Facebook without their consent and has not been destroyed. Plaintiff and Class Members have suffered harm and injury, including but not limited to the invasion of their privacy rights. Plaintiff continues to desire to be a patient of Geisinger and to have the ability to search for health information and treatment information on Geisinger's website. Plaintiff will continue to suffer harm if the website is not redesigned. If the website were redesigned to comply with applicable laws, Plaintiff would use the Geisinger website to search for health and treatment information in the future. Due to the continuing threat of injury,

Plaintiff and Class Members have no adequate remedy at law, and Plaintiff and Class Members are therefore entitled to injunctive relief.

WHEREFORE, Plaintiff on behalf of herself and her fellow Class Members respectfully requests this Honorable Court to enter judgment against Geisinger in excess of $1 million, together with all other compensatory, declaratory and injunctive relief, punitive damages, pre- and post-judgment interest, attorney's fees, costs of suit, and other such relief as the Court deems just and proper.

COUNT II
Invasion of Privacy—Intrusion Upon Seclusion
(On Behalf of Plaintiff and the Class)

340. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

341. Plaintiff brings this claim on behalf of herself and all members of the Class.

342. Pennsylvania law expressly recognizes that patients have a right to every consideration of privacy concerning their medical records. *See, e.g.,* 28 Pa. Code § 115.27; 49 Pa. Code § 16.61.

343. Geisinger intentionally intruded upon the private concerns of Plaintiff and Class Members in their personal health information.

344. Plaintiff and Class Members are current, former, or potential patients of Geisinger.

345. Geisinger owes Plaintiff and Class Members a duty of confidentiality.

346. Despite its duty not to disclose personal health information, Geisinger disclosed personal health information of Plaintiff and Class Members without their knowledge, consent, or authorization.

347. The information disclosed included personally identifiable information, Plaintiff and Class Members' statuses as patients of Geisinger, and the exact contents of communications

exchanged between Plaintiff and/or Class Members with Geisinger, including but not limited to information about treating doctors, potential doctors, conditions, treatments, appointments, search terms, bill payment, and logins to Geisinger's website.

348. Such disclosures constitute a substantial intrusion on the seclusion of Plaintiff's and Class Members' private concerns.

349. Geisinger's intentional disclosure of patients' personal health information to a third-party advertising company like Facebook without consent would be highly offensive to a reasonable person. Plaintiff and Class Members reasonably expected that their personal health information would not be collected, used, and monetized by third party advertising companies

350. Geisinger's disclosures of personal health information of Plaintiff and Class Members were highly offensive to a reasonable person at least because such disclosures violated expectations of privacy that have been established by the Pennsylvania Constitution, the Pennsylvania Patient's Bill of Rights, and established social norms. Privacy polls and studies show that Americans believe that one of the most important privacy rights is the need for an individual's affirmative consent before their personal data is collected, shared, or used.

351. Plaintiff and Class Members had a legitimate and reasonable expectation of privacy with respect to their personal health information and were accordingly entitled to protection of this information against the acquisition and disclosure of their personal health information by unreasonable means.

352. Geisinger owed a duty to Plaintiff and Class Members to protect the confidentiality of their personal health information and not to share such information with Facebook, Google, and others for marketing purposes without the express written consent of Plaintiff and Class Members.

353. Geisinger obtained Plaintiff's and Class Members' personal health information by falsely promising that it would safeguard the confidentiality of that information and that it would never disclose such information to third parties for marketing purposes without written consent. The deceitful method through which Geisinger obtained Plaintiff's and Class Members' personal health information (i.e., lying to patients about how their personal health information would be used) would be objectionable to a reasonable person.

354. The unauthorized acquisition, appropriation, and disclosure of Plaintiff's and Class Members' personal health information would also be highly offensive to a reasonable person.

355. The intrusion was into subject matter that was private and is entitled to be private. Plaintiff and Class Members disclosed their personal health information to Geisinger with the understanding that it would only be used for their medical treatment and that such information would be kept confidential and protected from disclosure to third parties. Plaintiff and Class Members reasonably believed that such information would be kept private and would not be shared with Facebook without their authorization so that Facebook could target them with advertising.

356. The disclosure of Plaintiff's and Class Members' personal health information by Geisinger constitutes an unreasonable intrusion upon Plaintiff's and Class Members' seclusion, as to both their persons, their private affairs, and private concerns of a kind that would be highly offensive to a reasonable person.

357. Geisinger acted with a knowing mind when it intentionally disclosed Plaintiff and Class Members' personal health information to Facebook, Google, and others. Geisinger further invaded Plaintiff's and Class Members' privacy by failing to implement adequate data security measures, despite its obligations to protect patients' personal health information.

358. Acting with knowledge, Geisinger had notice and knew that its disclosure of Plaintiff's and Class Members' personal health information would cause injury to Plaintiff and Class Members.

359. Given the nature of the personal health information that Geisinger disclosed to Facebook and others, such as patients' names, email addresses, phone numbers, information entered into forms, doctor's names, potential doctor's names, the search terms used to locate doctors (i.e. "Alzheimer's"), the condition selected from dropdown menus (i.e. "Heart Disease"), medications, and details about upcoming doctor's appointments, this kind of intrusion is both a substantial invasion of Plaintiff's and Class Members' privacy and would be (and in fact is) highly offensive to a reasonable person.

360. Geisinger's breach caused Plaintiff and Class Members, at minimum, the following damages:

a. Sensitive and confidential information that Plaintiff and Class Members intended to remain private is no longer private;

b. Geisinger eroded the essential confidential nature of the doctor-patient and provider-patient relationship;

c. Geisinger took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff and Class Members' knowledge, consent, or authorization and without sharing the benefit of such value;

361. Plaintiff and Class Members have suffered harm and injury, including but not limited to the invasion of their privacy rights.

362. Plaintiff and Class Members have been damaged as a direct and proximate result of Geisinger's invasion of their privacy and are entitled to seek just compensation, including monetary damages.

363. Plaintiff and Class Members seek appropriate relief for their injuries, including but not limited to damages that will reasonably compensate Plaintiff and Class Members for the harm to their privacy interests as well as a disgorgement of profits made by Geisinger as a result of its intrusions on Plaintiff and Class Members' privacy.

364. Plaintiff and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Geisinger's actions, which caused injury to Plaintiff and Class Members in conscious disregard of their rights. Such damages are needed to deter Geisinger from engaging in such conduct in the future.

365. Plaintiff and Class Members also seek such other relief as the Court may deem equitable, legal, and proper.

WHEREFORE, Plaintiff on behalf of herself and her fellow Class Members respectfully requests this Honorable Court to enter judgment against Geisinger in excess of $1 million, together with all other compensatory, declaratory and injunctive relief, punitive damages, pre- and post-judgment interest, attorney's fees, costs of suit, and other such relief as the Court deems just and proper.

COUNT III
Breach of Duty of Confidentiality
(On Behalf of Plaintiff and the Class)

366. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

367. Plaintiff brings this claim on behalf of herself and all members of the Class.

368. All conditions precedent to this action have been performed or occurred.

369. "Doctors have an obligation to their patients to keep communications . . . completely confidential." *Haddad v. Gopal*, 2001 PA Super 317, ¶ 5, 787 A.2d 975, 981 (Pa. Super. Ct. 2001).

370. As medical provider for Plaintiff and Class Members, Geisinger owes Plaintiff and Class Members a fiduciary duty of confidentiality in the data and content of communications exchanged between Geisinger and Plaintiff or Class Members.

371. Geisinger designed its website for patients to exchange communications with Geisinger relating to providers, treatment, billing, medical conditions, and patient records.

372. Geisinger's privacy policy assured Plaintiff and Class Members that Geisinger would protect the confidentiality of their personal health information and not use them for marketing purposes without written authorization.

373. Plaintiff and Class Members who paid money to Geisinger reasonably believed and expected that Geisinger would use part of those funds to operate its websites free of surreptitious collection and exploitation of communications between the parties. Geisinger failed to do so. Plaintiff and Class Members would not have purchased medical services from Geisinger if they knew that Geisinger would share their personal health information with Facebook, Google, and others without their knowledge or written consent.

374. Plaintiff and Class Members did not authorize, consent, know about, or take any action to indicate consent to Geisinger's conduct alleged herein.

375. Geisinger's conduct described herein was intentional.

376. Geisinger breached its duty of confidentiality by installing software code on its website that resulted in the disclosure of personal health information about Plaintiff and Class Members, including their status as patients, the content of their communications, and information

about their doctors, potential doctors, conditions, treatments, appointments, search terms, and bill payment to Facebook and other third parties.

377. Geisinger's breach caused Plaintiff and Class Members the following damages:

a. Sensitive and confidential information that Plaintiff and Class Members intended to remain private is no longer private;

b. Geisinger eroded the essential confidential nature of the doctor-patient and provider-patient relationship;

c. Geisinger took something of value from Plaintiff sand Class Members and derived benefit therefrom without Plaintiff and Class Members' knowledge, consent, or authorization and without sharing the benefit of such value;

d. Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Geisinger's duty to maintain the confidentiality of their personal health information; and

WHEREFORE, Plaintiff on behalf of herself and her fellow Class Members respectfully requests this Honorable Court to enter judgment against Geisinger in excess of $1 million, together with all other compensatory, declaratory and injunctive relief, punitive damages, pre- and post-judgment interest, attorney's fees, costs of suit, and other such relief as the Court deems just and proper.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

378. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

379. Plaintiff brings this claim on behalf of herself and all members of the Class.

380. Plaintiff and Class Members conferred a benefit on Geisinger in the form of valuable sensitive medical information that Geisinger collected from Plaintiff and Class Members under the guise of keeping this information private, and Geisinger appreciated this benefit.

381. Geisinger collected, used, and disclosed this information for its own gain, including for advertisement purposes, sale, or trade for valuable services from third parties. Additionally, Plaintiff and the Class Members conferred a benefit on Geisinger in the form of monetary compensation.

382. Plaintiff and the Class Members would not have used the Geisinger's services, or would have paid less for those services, if they had known that Geisinger would collect, use, and disclose this information to third parties.

383. Geisinger unjustly retained those benefits at the expense of Plaintiff and Class Members because Geisinger's conduct damaged Plaintiff and Class Members, all without providing any commensurate compensation to Plaintiff and Class Members.

384. The benefits that Geisinger derived from Plaintiff and Class Members rightly belong to Plaintiff and Class Members. It would be inequitable under unjust enrichment principles for Geisinger to be permitted to retain any of the profit or other benefits it derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

385. Geisinger should be compelled to disgorge in a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds that Geisinger received, and such other relief as the Court may deem just and proper.

WHEREFORE, Plaintiff on behalf of herself and her fellow Class Members respectfully requests this Honorable Court to enter judgment against Geisinger in excess of $1 million, together with all other compensatory, declaratory and injunctive relief, punitive damages, pre- and post-judgment interest, attorney's fees, costs of suit, and other such relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, asks for judgment in her favor, and that the Court enter an order as follows:

a. Certifying the Class and appointing Plaintiff as the Class's representative;

b. Appoint the law firms of Bochetto & Lentz, P.C., Simmons Hanly Conroy LLC, Don Bivens, PLLC, and Ahmad, Zavitsanos, & Mensing PLLC as class counsel;

c. Finding that Geisinger's conduct as alleged herein was unlawful;

d. Awarding such injunctive and other equitable relief as the Court deems just and proper, including enjoining Geisinger from making any further disclosure of Plaintiff or Class Members' communications to third parties without the Plaintiffs or Class Members' express, informed, and written consent;

e. Awarding statutory damages of $1,000 per Plaintiff and Class Members pursuant to 18 Pa. C.S.A. § 5725(a)(1);

f. Imposing a constructive trust against Geisinger through which Plaintiff and Class Members can be compensated for any unjust enrichment gained by Geisinger;

g. Awarding damages for violations of Plaintiff and Class Members' right to privacy;

h. Awarding Plaintiff and Class Members statutory, actual, compensatory, consequential, punitive, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;

i. Awarding Plaintiff and Class Members pre-judgment and post-judgment interest as provided by law;

j. Awarding Plaintiff and Class Members reasonable attorney's fees, costs, and expenses;

k. Awarding costs of suit; and

l. Such other and further relief to which Plaintiff and Class Members may be entitled.

RESPECTFULLY SUBMITTED,
COUNSEL FOR PLAINTIFF, INDIVIDUALLY AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED

George Bochetto, Bar. No. 27783
David P. Heim, Bar. No. 84323
Jane A. O'Connell, Bar. No. 205527
Ryan T. Kirk, Bar No. 329492
BOCHETTO & LENTZ, P.C.
1524 Locust St.
Philadelphia, PA 19102
Telephone: (215) 735-3900

Jay Barnes (*pro hac vice forthcoming*)
Eric Johnson (*pro hac vice forthcoming*)
SIMMONS HANLY CONROY
112 Madison Avenue, 7th Floor
New York, NY 10016
jaybarnes@simmonsfirm.com
ejohnson@simmonsfirm.com
Telephone: (212) 784-6400

Foster C. Johnson (*pro hac vice forthcoming*)
David Warden (*pro hac vice forthcoming*)
Weining Bai (*pro hac vice forthcoming*)
AHMAD, ZAVITSANOS, & MENSING, PLLC
1221 McKinney Street, Suite 2500
Houston, Texas 77010
fjohnson@azalaw.com
wbai@azalaw.com
dwarden@azalaw.com
Telephone: (713) 655-1101

Don Bivens (*pro hac vice forthcoming*)
DON BIVENS, PLLC
15169 N. Scottsdale Road, Suite 205
Scottsdale, Arizona 85254
don@donbivens.com
Telephone: (602) 708-1450

Dated: May 4, 2023

[redacted]

VERIFICATION

I, [redacted] hereby certify that I have read the foregoing and that the following is correct:

The facts set forth in the foregoing document are based upon information which I have furnished to counsel, as well as upon information which has been gathered by counsel and or/others acting on my behalf in this matter. The language of the document is that of counsel and not my own. I have read the document, and to the extent it is based upon information which I have given counsel, it is true and correct to the best of my knowledge, information and belief. To the extent the content of the document is that of counsel, I have relied upon such counsel in making this Verification. I hereby acknowledge that the facts set forth in the aforesaid document are made subject to the penalties of 18 Pa. C.S.A. §4904 relating to unsworn falsification to authorities.

5/1/2023 | 3:31 PM CDT

Date

[redacted]